4.8 Specialty Engineering

Specialty Engineering is a subset of System Engineering (SE) that defines and evaluates specific areas, features, and/or characteristics of a system. Specialty Engineering supplements the acquisition process by defining these characteristics and assessing their impact on the program. SE relies on specialty domain expertise to define and characterize specific requirements. SE's function in this process is to integrate the design engineer and specialty engineer's activities, coordinate and open communication lines between the design engineer and specialty engineer, and focus the engineering effort toward the common goal of satisfying the customer—not to perform detailed Specialty Engineering work.

Analysis of the system is a primary means of conducting Specialty Engineering. These analyses are categorized under Specialty Engineering because they require specialized engineering skills. These specialized skill areas include system safety engineering (SSE); Reliability, Maintainability, and Availability (RMA); Human Engineering (human factors); Electromagnetic Environmental Effects (E^3); quality Engineering; Information Security Engineering; and Hazardous Materials Management/Environmental Engineering. Engineers in these disciplines perform analyses throughout the system's lifecycle. The results are used to derive, validate, and verify requirements; evaluate system design progress and technical soundness; and manage risk. At a minimum, analysis results are available at standard design milestones, including the design, acquisition, and program reviews. The results are communicated via reports. In the case of supplier involvement, deliverables are in accordance with contract requirements. The general process for performing Specialty Engineering is depicted in Figure 4.8-1, which lists the key inputs necessary to initiate the task, providers, process tasks, outputs required, and customers of process outputs.

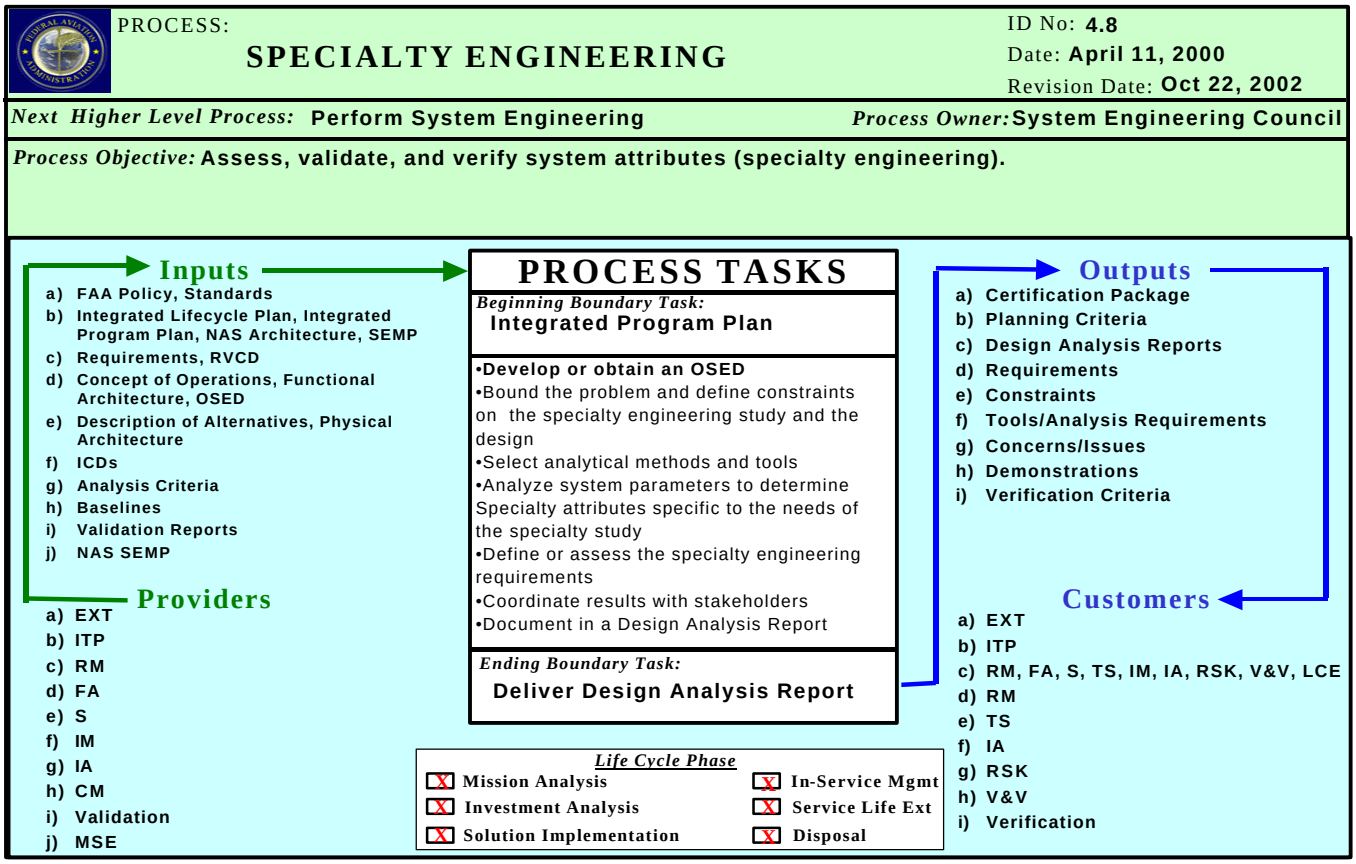


Figure 4.8-1. Specialty Engineering Process-Based Management Chart

4.8.0 Introductory Material

4.8.0.1 Introduction to Specialty Engineering

Specialty Engineering is conducted throughout the system's lifecycle. Specialty Engineering analyses are conducted early to derive and validate requirements. In addition, the Specialty Engineering disciplines support the Trade Studies (Section 4.6), Synthesis (Section 4.5), and Functional Analysis (Section 4.4) efforts in selecting and designing solutions to requirements. Later in the lifecycle, after requirements at all levels are validated, these analyses provide support in verifying the requirements by describing and assessing the characteristics of the design and/or operations. As early as possible in the lifecycle, the Specialty Engineering disciplines find and resolve potential program risk. Finding and controlling risk early assists in seeking the lowest possible cost and increases the probability of program success and operator acceptance of the product.

This section contains a description of the functions, objectives, and products of the various disciplines included in Specialty Engineering.

4.8.0.1.1 Description of Specialty Engineering Disciplines

Specialty Engineering analyses provide characteristics of the system from a specific technical perspective. Table 4.8-1 provides a general description of the Specialty Engineering disciplines.

Table 4.8-1. Specialty Engineering Disciplines

Specialty Engineering Discipline	Description
SSE	Evaluation and management of the safety risk associated with a system using measures of safety risk identified in various hazard analyses, fault tree analyses, safety risk assessments, and hazard tracking and control.
RMA	Quantitative and qualitative analyses of the attributes of the system to perform reliably. Quantitative assessments are in the form of probabilistic, mean, and/or distribution assessments. Qualitative analyses are in the form of failure mode assessments. Evaluation of the design's ability to meet operational readiness requirements through preventive and corrective maintenance.
Human Factors Engineering	Human factors is a multidisciplinary effort to generate and compile information about human capabilities and limitations and apply that information to: – equipment, systems, facilities – procedures, jobs, environments – staffing – training – personnel and organizational management for safe, comfortable, and effective human performance.
E^3	Analysis of the system for susceptibility and/or vulnerability to electromagnetic fields or capability to generate such fields that might interfere with other systems, identify sources of interference, and means for correction within the levels prescribed by law, program requirements, spectrum management, or recognized standards. E^3 is composed of Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC)
Quality Engineering	Evaluation of a system's ability to meet its requirements and to mitigate product defects.
Information Security Engineering (ISE)	Applies scientific and engineering principles to manage and control system security risk to the enterprise and its mission. Risk identification includes identifying system vulnerabilities and threats. ISE applies effective and suitable technical, procedural, physical,

Specialty Engineering Discipline	Description
	and administrative controls to mitigate these risks to an acceptable level. ISE combines control measures for prevention, detection, and recovery from security attacks that would compromise confidentiality, integrity, and/or availability of information technology assets (including information).
Hazardous Materials Management/Environmental Engineering	Determination of environmental impacts at deployment sites and during operations, including both environmental impacts on the system and system impacts on the environment during all phases of the product life.

In addition to resolving problems and defining requirements early, Specialty Engineering supplies information to the other SE functions, including Requirements Management (Section 4.3), Risk Management (Section 4.10), Configuration Management (Section 4.11), and Validation and Verification (Section 4.12). The major relationships between Specialty Engineering and other SE processes are depicted in Figure 4.8-2.

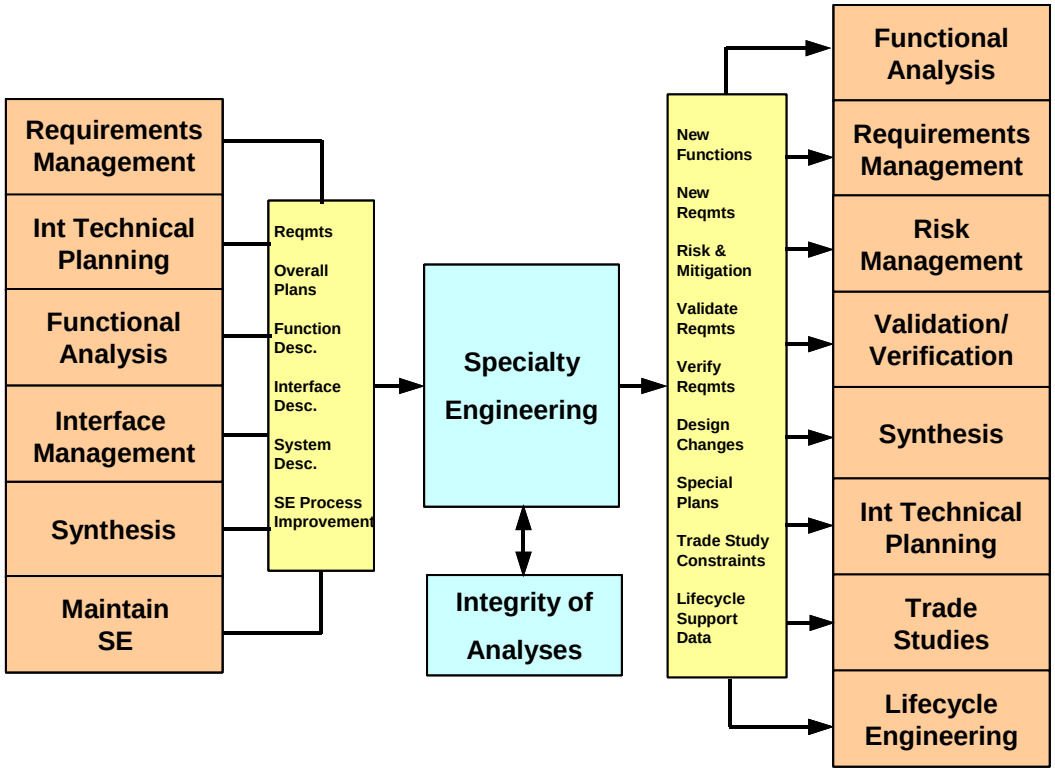


Figure 4.8-2. Major Relationships Between System Engineering Elements and Specialty Engineering

The relationships depicted in Figure 4.8-2 are further described in Table 4.8-2.

Table 4.8-2. Major Effects of Specialty Engineering on Other System Engineering Processes

Affected SE Process	How Affected
Integrated Technical Planning (Section 4.2)	The Integrated Technical Planning process feeds Specialty Engineering. Integrated Technical Planning produces the plans for Specialty Engineering, SE, and all other SE processes. The plans detail what is to be done, who is to do it, the standards of performance, and when each task is to be performed.
Requirements Management (Section 4.3)	The Requirements Management process both feeds and is fed by Specialty Engineering. The system under study is described in order to perform Specialty Engineering analyses. Requirements are a key component of any description and they are an output of the Requirements Management process. Specialty Engineering studies often find characteristics that create a need for new or different requirements. Sometimes, the Specialty Engineering disciplines find areas of conflict between two or more requirements. In either case, the Specialty Engineering function develops the new or changed requirements and these are an input to the Requirements Management process.
Functional Analysis (Section 4.4)	The Functional Analysis process both feeds and is fed by Specialty Engineering. To execute a Specialty Engineering analysis, the specialist shall have a thorough understanding of the system functions. This understanding is a result of performing a Functional Analysis of the system.
Interface Management (Section 4.7)	Specialty Engineering both feeds and is fed by Interface Management. The system under study is described in order to perform Specialty Engineering analyses. Interface Requirements Descriptions (IRD) are key components of any system description and are an output of the Interface Management process. Specialty Engineering studies often find characteristics that create a need for new or different interface requirements or descriptions. Sometimes, the Specialty Engineering disciplines find areas of conflict between two or more interfaces. In either case, the Specialty Engineering function develops the new or changed requirements, which are inputs to the Interface Management process.
Risk Management (Section 4.10)	Specialty Engineering feeds the Risk Management process. Specialty Engineering studies and analyses are designed to find and assess potential problem areas of a design as early as possible. When a potential problem is found, the information becomes an input to the Risk Management process for mitigation and control.
Configuration Management (Section 4.11)	Specialty Engineering outputs are inputs to the Configuration Management process. During the execution of Specialty Engineering analyses, it may be discovered that additional or changed design features are required, or changes to operating, maintenance, or installation procedures are needed. When these discoveries occur, the proposed changes become inputs to the Configuration Management process.

Affected SE Process	How Affected
Validation and Verification (Section 4.12)	Specialty Engineering outputs feed the Validation and Verification process. Early in the program's lifecycle, Specialty Engineering is used to validate requirements, which is accomplished by comparing the requirements defined in early Specialty Engineering analyses to those defined in current/later analyses. If the Specialty Engineering analyses find a need for an existing requirement, then the requirement may be considered validated. Specialty Engineering feeds Verification Criteria to the Verification process. Specialty Engineering is also used to verify requirements later in the system's lifecycle. Verification may be accomplished either by test or SE Assessment. Specialty Engineering is a form of assessment and may be used to demonstrate verification.

4.8.0.2 Inputs and Providers to Specialty Engineering

Table 4.8-3 depicts the inputs needed to conduct Specialty Engineering analyses.

Table 4.8-3. Specialty Engineering Process Inputs

Process Input	Input Purpose/Description	From Process
FAA Policy and Standards	Policy and standards, such as the Acquisition Management System (AMS), define what is expected and how well it needs to be done.	AMS and FAA Orders
Integrated Lifecycle Plan	The Integrated Lifecycle Plan provides planning information necessary to support the system throughout its lifecycle.	Integrated Technical Planning (Section 4.2)
Integrated Program Plan (IPP)	The IPP provides information on the overall plan for conducting the program. It provides information on program constraints, system constraints, and Specialty Engineering plans. Each specific program maintains the IPP. It is an aggregate plan that includes and integrates all the program specific plans. The IPP details what tasks are to be performed, who is to do them, and when the tasks are to be performed.	Program's IPP Integrated Technical Planning (Section 4.2)
National Airspace System (NAS) Architecture	The NAS Architecture is the technical blueprint for NAS Modernization and guides the Federal Aviation Administration (FAA) on what systems are planned for modernizing the NAS.	Synthesis (Section 4.5)

Process Input	Input Purpose/Description	From Process
System Engineering Management Plan (SEMP)	The SEMP defines the plan for conducting SE in the AMS and the program.	System Engineering in the Acquisition Management System Program Lifecycle (Chapter 3)
Requirements	Requirements provide information about the system's required characteristics, specifications, performance, and requirements. They assist in developing the system description. System requirements are documented in the initial Requirements Documents (iRD), final Requirements Documents (fRD), and system specification(s). The execution teams and SE develop and maintain the requirements documents.	Requirements Management (Section 4.3)
Requirements Verification Compliance Documents (RVCD)	The RVCD records the verification status of all requirements.	Requirements Management (Section 4.3)
Concept of Operations (CONOPS)	The CONOPS is a user-oriented document that describes system functional characteristics for a proposed system from the user's viewpoint. It explains the existing system, current environment, users, interactions among users and the system, and organizational impacts. The CONOPS document is written in order to communicate overall quantitative and qualitative system characteristics to the user, buyer, developer, and other organizational elements.	Functional Analysis (Section 4.4)
Functional Architecture	The Functional Architecture identifies, analyzes, and describes the functions of a system. It provides information required for a system description and assists in the definition of requirements. Functional Analysis is the process of turning a need or system requirement into a description and an architecture of functions (system behaviors or behavior descriptors). The execution teams and/or SE perform and maintain the Functional Architecture.	Functional Analysis (Section 4.4)

Process Input	Input Purpose/Description	From Process
Operational Services and Environmental Description (OSED)	The OSED is a comprehensive, holistic Communications, Navigation, and Surveillance (CNS)/Air Traffic Management (ATM) system description. It describes the services, environment, functions, and mechanizations that form a system's characteristics.	Functional Analysis (Section 4.4)
Description of Alternatives	Description of Alternatives is described as Physical Architectures. When performing Trade Studies (Section 4.6), a number of alternatives shall be competitively evaluated.	Synthesis (Section 4.5)
Physical Architecture	Physical Architecture identifies and defines the system and its components, including the physical interfaces among products, subsystems, humans, lifecycle processes, and external interfaces to higher-level systems or interacting systems.	Synthesis (Section 4.5)
Interface Control Document (ICD)	The ICD contains and documents the "as built" interface design derived from the IRD.	Interface Management (Section 4.7)
Analysis Criteria	Criteria for specialty engineering analyses are specified to establish the degree of validation required for the analyses and associated tools, the methods to use to ensure that the data is of the proper quality and range, and the level of documentation required.	Integrity of Analysis (Section 4.9)
Baselines	When the requirements and design have reached sufficient maturity, they are baselined to facilitate management of the configuration.	Configuration Management (Section 4.11)
Validation Reports	Validation Reports document the results of the Validation effort. They report requirements that are validated and those that are considered nonconforming.	Validation (Section 4.12)
NAS SEMP	The NAS SEMP describes the overall SE used in the FAA.	Manage System Engineering (Section 4.14)

4.8.0.3 General Specialty Engineering Process Tasks

Most, if not all, Specialty Engineering disciplines follow a similar process during the conduct of associated analyses. The following paragraphs provide general guidance on performing Specialty Engineering in the FAA. These processes are depicted in Figure 4.8-1. The process tasks are:

- Describe the system in physical and/or functional terms. This task has to be completed before the specialists may begin; if not, the specialists may perform this task, as long as it is performed according to the guidance in Functional Analysis (Section 4.4) and Interface Management (Section 4.7)).
- Bound the problem and define Constraints on the Specialty Engineering study and the design.
- Select analytical methods and tools.
- Analyze system parameters to determine specialty attributes specific to the views of the Specialty Engineering study.
- Define or assess the Specialty Engineering Requirements.
- Coordinate results with stakeholders.
- Document the analysis in a Design Analysis Report (DAR).

The following paragraphs detail the process tasks depicted in Figure 4.8-1.

4.8.0.3.1 Task 1: Obtain or Develop an Operational Services and Environmental Description

The first task in performing a Specialty Engineering analysis is to understand and describe the system under study at an appropriate level. The OSED is an excellent source of this information; it is a system description that is developed in the Functional Analysis process (Section 4.4).

It is recommended that the specialty engineer use the existing descriptions to frame the Specialty Engineering analysis. However, there are times when the existing system descriptions are insufficient in detail for the specialist. In these cases, the specialty engineer develops the system description. When developing the system description, the specialty engineer shall comply with the guidance in Functional Analysis and Interface Management (Section 4.7).

Functional Analysis describes the desired behaviors of a system. These behaviors provide critical insight into how the system is intended to perform and, therefore, are a critical input to any Specialty Engineering analysis. To perform an assessment of a system, the engineer is required to understand the functions of that system and be able to relate the specialties to these functions. Normally, the Functional Analysis is completed before the Specialty Engineering process begins, and all that is required of the specialty engineer is to obtain and review the Functional Analysis and use it to enhance or complete the system description. In some cases, either because the engineers failed to perform it or because it is too early in the design process, the Functional Analysis is not available. In these cases, the specialty engineer shall refer to guidance in Functional Analysis and perform the Functional Analysis independently.

4.8.0.3.2 Task 2: Bound the Problem and Define Constraints on the Study and Design

Every system problem or analysis has breadth and depth. The breadth of a system analysis refers to the system boundaries. Boundaries limit the system to elements of the system model that affect or interact with each other in order to accomplish the central mission(s) or function. Depth refers to the level of detail in the description. The level of detail in an analysis varies inversely with the breadth of the system. For a system as broad as the NAS, the description

and analysis are general in nature with little detail on individual components. On the other hand, a simple system, such as a valve in a landing gear design, includes significant detail to support the assessment.

Constraints on the design play an important role in the conduct of the analysis and the credibility of the results. It is essential to identify the Constraints before the analysis to account for their influence on the methods used and the alternatives chosen. As part of determining the Constraints, the scope of the analysis, the ground rules, and assumptions are identified. Identifying the customer(s) for the analysis is important with respect to defining the scope. The analysis may be subject to contractual restraints if it is a deliverable; therefore, it is necessary to consider these restraints when defining the scope of the effort. The project schedule and budget may also impose limits on the analysis, which may affect the assumptions and ground rules. The analysis team and the recipients of the report shall be aware of all the scope limitations, ground rules, assumptions, and guidelines that apply to the assessment and product design. The following sources are used to identify Constraints:

- CONOPS defined via Functional Analysis (Section 4.4)
- Contract Statement of Work (SOW), including referenced standards and procedures
- Compliance documents that apply to the analysis methods and report
- Customer-specified requirements on cost, schedule, and product performance
- Management-imposed business goals and Constraints
- Functional, performance, and interface requirements derived from the design concept
- Functional, performance, and interface requirements imposed by the use of commercially available or preexisting hardware and software
- Operational constraints imposed by the user
- Environmental constraints imposed by the physical and operational environment
- Constraints imposed by the production or Verification process (Section 4.12)
- Design constraints imposed by standard practices that are defined by the government or standards-setting bodies
- Federal, Department, and FAA policies, standards, and guidelines

4.8.0.3.3 Task 3: Select Analytic Methods and Tools

To ensure Integrity of Analyses (Section 4.9), the engineer selects analytic methods and tools that meet the program phase; the system analysis needs; and cost, schedule, and skill constraints. It is important to select methods and tools that match the analysis objectives within the resource limitations of the effort.

4.8.0.3.4 Task 4: Analyze System Parameters To Determine System Attributes

In this step, the attributes of the design are determined by using the methods and tools appropriate to the Specialty Engineering discipline. The appropriate guidelines and handbooks for each Specialty Engineering discipline are listed in Table 4.8-4. The AMS FAA Acquisition System Toolset (FAST) often contains guidelines for these activities. For example, it is recommended that the team, if conducting a safety assessment, consult the FAA System Safety

Handbook (SSH) and the NAS System Safety Management Plan (SSMP) found in the FAST. For some analyses, it is recommended that the results include programmatic attributes, such as cost and schedule impacts, as appropriate to the analysis.

In addition, the SE or project team, as part of this process, conducts technical or peer reviews of the analysis and its results. The technical community conducts this independent evaluation before the Specialty Engineering DARs are submitted.

The results of Specialty Engineering analyses confirm design attributes necessary for acceptable product performance, cost, schedule, and risk. When an attribute is not confirmed, the analysis and/or the baseline shall be revised.

Revision may be implemented through changes in scope, ground rules, assumptions, and analytic methods. The analysis process is reactivated with the intent of determining an alternative result that is acceptable and valid. Alternatively, the results of the analysis may drive revision of the Requirements or design Baseline. This revision is accomplished by preparing appropriate change proposal documentation for input to the Configuration Management process (Section 4.11).

Table 4.8-4. Guidelines and Handbooks for Conducting Specialty Engineering

Phase	Analysis	Guidance/Reference
Mission Analysis	E^3 EMC requirements	FAST. (2000). Environment/Energy/ Safety/Health. http://fast.faa.gov/ FAST. (2000). Radio Spectrum Management. http://fast.faa.gov/
	Environmental Requirements Analysis	FAST.[1] Environment/Energy/Safety /Health. http://fast.faa.gov/
	Human Factors Functional Analysis	FAST. Human Factors. http://fast.faa.gov/
	Human Factors System (Mission) Analysis	FAST. Human Factors. http://fast.faa.gov/

[1] Federal Aviation Administration, Federal Acquisition System Tools (FAST), Office of Research and Acquisitions (ARA), [On-line] Available: http://fast.faa.gov.

Phase	Analysis	Guidance/Reference
	Maintainability Requirements Analysis	FAST. Sustainment and Maintenance. http://fast.faa.gov/
	Operational Safety Assessment (OSA)	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH[2], Chapter 4. NAS SSMP[3], Chapters 3 and 4.
	Reliability Requirements Analysis	(Reserved)
	Information Security Engineering	Preliminary Risk Assessment, Guidance/Reference: FAA ISS Handbook 1370.82
Investment Analysis	Comparative Safety Assessment (CSA)	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 4 NAS SSMP
	EMC Control Plan	FAST. (2000). Environment/Energy/ Safety/Health. http://fast.faa.gov/ FAST. (2000). Radio Spectrum Management. http://fast.faa.gov/
	Human Factors Function Allocation	FAST. Human Factors. http://fast.faa.gov/
	Human Factors Program Plan	FAST. Human Factors. http://fast.faa.gov/
	Maintainability Plan	FAST. Sustainment and Maintenance. http://fast.faa.gov/
	Preliminary Hazard Analysis (PHA)	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 8 NAS SSMP
	Quality Engineering Plan	FAST. Quality Assurance. http://fast.faa.gov/
	Reliability Program Plan	(Reserved)

[2] U.S. Federal Aviation Administration, "FAA System Safety Handbook," FAA Office of System Safety (ASY), Washington, DC (2000).

[3] U.S. Federal Aviation Administration, "NAS Modernization System Safety Management Plan," FAA Office of Architecture and SE (ASD), Washington, DC (2000).

Phase	Analysis	Guidance/Reference
	Specialty Engineering Support of Trade Studies or Alternatives Analysis	FAST. Investment Analysis. http://fast.faa.gov/ Synthesis of Alternatives (Section 4.8)
	System Safety Program Plan (SSPP)	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 5 NAS SSMP
	Information Security Engineering	Updated Risk Assessment, Guidance/Reference: FAA ISS Handbook 1370.82
Solution Implementation	Environmental/ Hazardous Material Analysis	FAST. Environment/Energy/Safety /Health. http://fast.faa.gov/
	Failure Modes and Effects Analysis (FMEA)	(Reserved)
	Failure Modes and Effects Criticality Analysis (FMECA)	(Reserved)
	Failure Reporting Analysis and Corrective Action System (FRACAS)	(Reserved)
	Failure Review Board	(Reserved)
	Hazard Tracking and Risk Resolution	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 3 NAS SSMP
	Human Factors Demonstrations, Models, and Mockups	(Reserved)
	Human Factors Error Analysis	(Reserved)
	Human Factors Operational Sequence Diagrams	(Reserved)
	Human Factors Operator Task Analysis	(Reserved)
	Human Factors Timeline Analysis	(Reserved)
	Human Factors Workload Analysis	(Reserved)

Phase	Analysis	Guidance/Reference
	Maintainability Analysis	FAST. Sustainment and Maintenance. http://fast.faa.gov/
	Maintainability Demonstration	FAST. Sustainment and Maintenance. http://fast.faa.gov/
	Maintainability Modeling	FAST. Sustainment and Maintenance. http://fast.faa.gov/
	Maintenance Task Analysis	FAST. Sustainment and Maintenance. http://fast.faa.gov/
	Operating and Support Hazard Analysis (O&SHA)	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 8 NAS SSMP
	Reliability Centered Maintenance (RCM)	(Reserved)
Solution Implementation	Reliability Development Growth Testing (RDGT)	(Reserved)
	Reliability Modeling	(Reserved)
	Sneak Circuit Analysis	(Reserved)
	Subsystem Hazard Analysis (SSHA)	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 8 NAS SSMP
	System Hazard Analysis (SHA)	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 8 NAS SSMP
	Information Security Engineering	Analysis supporting Certification and Authorization, Guidance/Reference: FAA ISS Handbook 1370.82

4.8.0.3.5 Task 5: Define and Document Specialty Engineering Requirements

The Specialty Engineering products described in “Task 4: Analyze System Parameters to Determine System Attributes” (Paragraph 4.8.0.3.4) result in the definition and assessment of Specialty Engineering-related Requirements. These Requirements shall meet the standards for requirements definition and documentation described in Requirements Management (Section 4.3). In addition, these Requirements shall be validated and verified, as described in Validation and Verification (Section 4.12).

4.8.0.3.6 Task 6: Coordinate Results With Stakeholders

The results of the Specialty Engineering process (particularly the DARs and Requirements) shall be coordinated with the project/program stakeholders. This coordination is conducted in both formal and informal forums. The informal forums include peer reviews and working groups.

The formal forums include Acquisition Reviews and Design Reviews, as described in Integrated Technical Planning (Section 4.2).

4.8.0.3.7 Task 7: Document the Specialty Engineering Analysis in a Design Analysis Report

The primary output of any Specialty Engineering function is the DAR, which documents the results of the specific analysis with rationale. Each DAR shall contain the following results:

- Description of the system's special characteristics
- List of existing Requirements that were either validated or verified in the analysis
- Residual risks
- Candidate Requirements found as a result of the analysis

These Requirements are inputs to the Requirements Management process (Section 4.3) and shall be considered for inclusion in iRD and fRD. The rationale includes the scope, ground rules, assumptions, constraints, methods, and tools applicable to the analysis.

The Specialty Engineering outputs are often used to validate and/or verify requirements. In addition, change proposal documentation is produced if the conclusions of the analysis call for a revision to the Requirements or design Baseline. This revision is an input to the Configuration Management process (Section 4.11) for authorization to change the Baseline as the analysis indicates.

Requirements for contents and format may be applicable to the DAR as specified by the contract. Figure 4.8-3 provides a sample outline of the contents of the DAR.

1.0 Executive Summary
2.0 Introduction
3.0 Summary of results
4.0 Summary of conclusions (including residual risks)
5.0 Recommendations (including mitigation)
6.0 System Description
  6.1 Summary
  6.2 Operational Services and Environment Description (OSED)
  6.3 Functional Analysis (if applicable)
  6.4 Requirements (if applicable)
7.0 Description of system special characteristics (detailed analysis worksheets or data)
8.0 List of candidate requirements
9.0 List of requirements that were validated and/or verified with rationale
10.0 Analysis methodology with rationale

Figure 4.8-3. Sample Outline of a Design Analysis Report

4.8.0.4 Outputs of Specialty Engineering

The following paragraphs describe the outputs of Specialty Engineering. The outputs are:

- Certification Package
- Planning Criteria
- DARs (specific to the Specialty Engineering study)
- Specialty Engineering Requirements
- Constraints
- Tools/Analysis Requirements
- Concerns/Issues
- Demonstrations
- Verification Criteria

4.8.0.4.1 Certification Package — Reserved

4.8.0.4.2 Planning Criteria

Any Planning Criteria necessary for performing Specialty Engineering throughout the remainder of the program's lifecycle need to be provided to the Integrated Technical Planning process (Section 4.2)

4.8.0.4.3 Design Analysis Report

The DAR is the means of documenting and reporting the methods and results of the Specialty Engineering analyses. Figure 4.8-3 provides a sample outline of a DAR.

4.8.0.4.4 Specialty Engineering Requirements

In the course of performing an analysis, the specialty engineer typically defines, validates, or verifies Requirements. Occasionally, the specialist discovers characteristics of the system that are not adequately specified in the existing Requirements or specification documents. If this occurs, the specialist defines those necessary Requirements consistent with the specialist's area of expertise and the requirements standards described in Requirements Management (Section 4.3).

4.8.0.4.5 Constraints

Constraints necessary for performing Specialty Engineering throughout the remainder of the program's lifecycle need to be provided to the Trade Studies process (Section 4.6).

4.8.0.4.6 Tools/Analysis Requirements

Tools/Analysis Requirements for performing Specialty Engineering throughout the remainder of the program's lifecycle need to be provided to the Integrity of Analyses process (Section 4.9).

4.8.0.4.7 Concerns/Issues

Appendix D contains guidance on Concerns/Issues as a product of Specialty Engineering.

4.8.0.4.8 Demonstrations

Demonstrations are often used to verify compliance with Requirements in servicing, reliability, maintainability, transportability, and human factors engineering. Demonstrations are used to verify what is accomplished by operating, adjusting, or reconfiguring items performing their design functions under specific scenarios. The items may be instrumented and quantitative limits of performance monitored; however, only check sheets are required rather than recordings of actual performance data. This method is used when actual demonstration techniques may be used to verify compliance with a Requirement. Observations made by engineers or instrumentation are compared with predetermined responses based on the requirements. An example of this verification method is the demonstration of installing and uninstalling an aircraft engine in a required amount of time.

Demonstrations may also be used to validate unstable Requirements. If there is a risk inherent to a Requirement, Demonstrations may be used to determine the correct characteristics needed.

"Test and Evaluation Verification" (Paragraph 4.12.2.2.1,Verification by Demonstration) has more information on Demonstrations.

4.8.0.4.9 Verification Criteria

The specialist may be called upon to define specific verification requirements, as described in "Step 3: Develop Verification Approach" (Paragraph 4.12.2.5.2.2.3). The Verification Criteria or requirements are added to the Verification Requirements Traceability Matrix (VRTM).

4.8.0.5 Specialty Engineering Tools

The tools used in Specialty Engineering are often unique to each Specialty Engineering discipline. They include databases, drawing tools, requirements and Functional Analysis tools, word and document processors, and spreadsheets. The selection of specific tools depends on criteria established by the particular program. These tools are identified and controlled as documented in individual Specialty Engineering plan sections of the IPP.

4.8.0.6 Specialty Engineering Process Metrics

The schedule completion of Specialty Engineering analyses measured against the plan is a measure of the degree to which these analyses are being effectively managed. The effectiveness of Specialty Engineering analyses may be measured by the rework of analyses or incompatibility with measured performance as an indication that these analyses are reaching inaccurate conclusions.

Of the seven general measurement categories discussed in this section, the five that are applicable to Specialty Engineering are Schedule and Progress, Resources and Cost, Process Performance, Customer Satisfaction, and Product Quality. These measures, along with other candidate measures for Specialty Engineering, are provided in Table 4.8-5. It is recommended that each effort tailor these measures and add other applicable project-specific measures to ensure the contribution of necessary information to the decisionmaking processes.

Table 4.8-5. Candidate Measures for Specialty Engineering*

Schedule and Progress	Resources and Cost	Product Size and Stability	Product Quality	Process Performance	Technology Effectiveness	Customer Satisfaction
Achievement of specific milestone dates	Total effort compared to plan	Documentation of special engineering characteristics	Technical performance	Process productivity	Technology impact on product	Customer survey results
Test status	Resource utilization	Requirements	Defects	Process activity cycle time	Baseline changes	Performance rating
Percent of analysis studies completed (schedule and progress)		Percent of requirements derived from specialty analyses	Standards compliance	Depth of the specialty analyses as a percentage versus the target depth		

*NOTE: The measures above are only general examples to indicate the type of information that might be included in the individual section measurement matrix.

4.8.1 System Safety Engineering

SSE (also called Safety Risk Management) is a Specialty Engineering discipline within SE. It is recommended that system/safety engineers and program managers refer to the FAA SSH and the NAS Modernization SSMP for detailed information regarding the planning and conduct of SSE. The following paragraphs describe how system safety is integrated into a system's overall SE.

4.8.1.1 What Is System Safety Engineering?

SSE is the application of engineering and management principles, criteria, and techniques to optimize the safety of a system within the program's operational and programmatic constraints. These engineering and related management tools are used to identify, evaluate, and control hazards associated with a system. A hazard is a real or likely event that has the potential to harm people or damage the system. SSE's goal is to identify the hazards in a system early and continuously to assess the risk (severity and likelihood) of each hazard and to actively control the highest risk hazards. The NAS Modernization SSMP, Figure 4.2-1 (Risk Assessment Matrix) under the Safety Risk Management hyperlink in the FAST (http://fast.faa.gov/toolsets/index.htm), provides more information on this topic, as do Table 4.2.1 (Severity Definitions) and Table 4.2-2 (Likelihood or Probability Definitions).

As illustrated in Figure 4.8-4, the SSE process is a closed-loop method of Risk Management (Section 4.10).

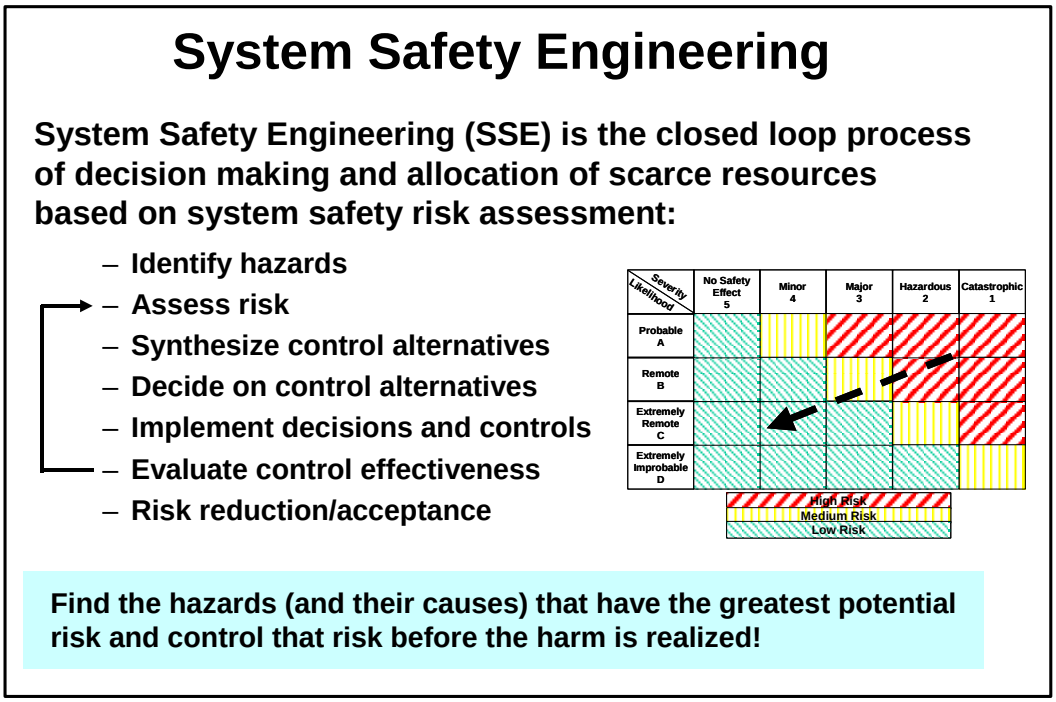


Figure 4.8-4. Closed-Loop Nature of System Safety Engineering

To conduct SSE in the AMS, the program performs hazard analyses, as described in the NAS SSMP, Chapters 4 and 5 (http://fast.faa.gov/toolsets/index.htm), and the SSH, Chapter 8 (http://fast.faa.gov/toolsets/index.htm). Figure 4.8-5 shows what safety analyses are performed relative to the phases and decisions of the Integrated Product Development System of the AMS. These safety analyses are timed to best support the phased needs and decisions in the overall AMS process.

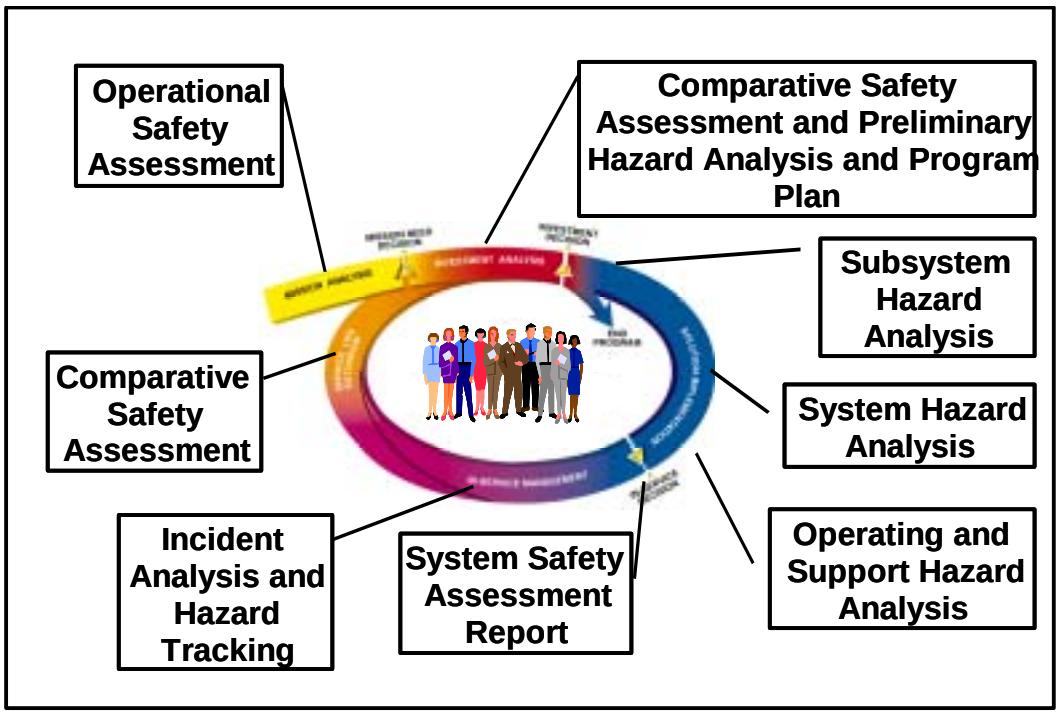


Figure 4.8-5. Types of Safety Hazard Analyses and Their Relative Position in the Acquisition Management System

4.8.1.2 Why Perform System Safety Engineering?

There are two basic reasons for performing SSE on a program:

- To comply with FAA Orders and AMS direction (e.g., FAA Order 8040.4 and AMS, Paragraph 2.9.13)
- To reduce total cost of development and improve program integration

The FAA's primary role is to ensure the safety of the NAS. In performing this role, the FAA has issued FAA Order 8040.4 (http://fast.faa.gov/toolsets/index.htm), which directs all FAA organizations to employ safety risk management in decisionmaking. The AMS was amended to

comply with FAA Order 8040.4. The AMS now requires programs to execute system safety and to brief the system safety program status at all Joint Resources Council (JRC) meetings and Acquisition Reviews. The SSH, Chapter 2 (http://fast.faa.gov/toolsets/index.htm), the SSMP, Chapter 6 (http://fast.faa.gov/toolsets/index.htm), and the AMS provide more information on this subject. For example, AMS Paragraph 2.9.13 reads:

> *System Safety Management shall be conducted and documented throughout the acquisition management lifecycle. Critical safety issues identified during mission analysis are recorded in the Mission Need Statement; a system safety assessment of candidate solutions to mission need is reported in the Investment Analysis Report; and Integrated Product Teams provide for program-specific safety risk management planning in the Acquisition Strategy Paper.*

Each line of business involved in acquisition management shall institute a system safety management process that includes, at minimum, the following:

- Hazard identification
- Hazard classification (severity of consequences and likelihood of occurrence)
- Measures to mitigate hazards or reduce risk to an acceptable level
- Verification that mitigation measures are incorporated into product design and implementation
- Assessment of residual risk

Status of system safety shall be presented at all JRCs. The FAST provides detailed guidelines for system safety management (http://fast.faa.gov/toolsets/SafMgmt/IndexStart.htm).

The second reason for conducting safety risk management is that it reduces cost and improves system integration and SE overall.

- System safety looks for programmatic risks that may impact system performance, schedule, and costs.
- System safety finds problems early. As Figure 4.8-6 shows, the earlier in the lifecycle a problem is found and managed, the easier and less expensive it is to correct.

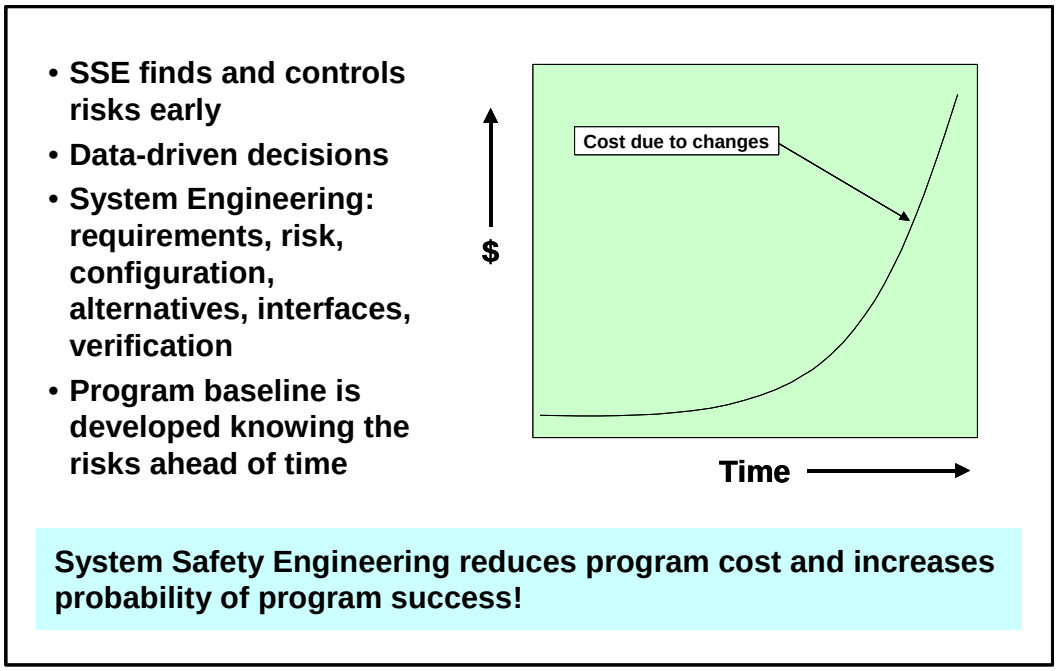


Figure 4.8-6. Benefits of System Safety Engineering

- The outputs of the system safety process feed other SE processes, improving the overall SE of the system (Figure 4.8-7).

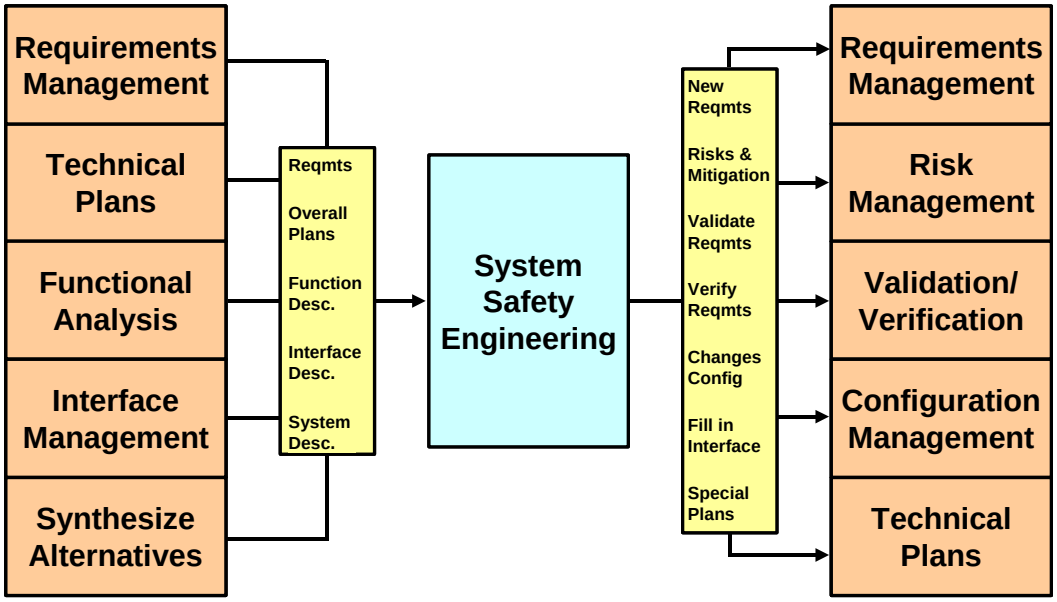


Figure 4.8-7. System Safety Engineering's Relationship to Other System Engineering Processes

4.8.1.3 System Safety Engineering Process Tasks

SSE follows the process tasks outlined in "General Specialty Engineering Process Tasks" (Paragraph 4.8.0.3).

4.8.1.4 System Safety Engineering Outputs/Products

The following products are outputs of SSE.

4.8.1.4.1 Program Planning

Each program is required to have an SSPP. The NAS Modernization SSMP (http://fast.faa.gov/toolsets/index.htm) is the overall plan for conducting safety risk management in the AMS. It is recommended that individual programs consult the SSMP when developing a program-specific SSPP that meets the NAS SSMP requirements. The FAA SSH, Chapter 5 (http://fast.faa.gov/toolsets/index.htm), also provides guidance on this topic.

4.8.1.4.2 Analysis Products

Table 4.8-6 lists the products of SSE. Detailed directions for how to develop these products are referenced in the table.

386 **Table 4.8-6. Products of System Safety Engineering**

System Safety Process Products	How To Reference
Operational Safety Assessment (OSA)	FAA SSH, Chapters 2 and 4 (http://fast.faa.gov/toolsets/index.htm) NAS SSMP, Section 5.2.1 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.1)
Comparative Safety Assessment (CSA)	FAA SSH, Chapters 2 and 4 NAS SSMP, Section 5.2.2 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.2)
Preliminary Hazard Analysis (PHA)	FAA SSH, Chapter 8 NAS SSMP, Section 5.2.3 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.3)
System Safety Program Plan (SSPP)	FAA SSH, Chapter 5 NAS SSMP, Section 5.2.4 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.4)
Subsystem Hazard Analysis (SSHA)	FAA SSH, Chapter 8 NAS SSMP, Section 5.2.5 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.5)
System Hazard Analysis (SHA)	FAA SSH, Chapter 8 NAS SSMP, Section 5.2.6 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.6)
Operating and Support Hazard Analysis (O&SHA)	FAA SSH, Chapter 8 NAS SSMP, Section 5.2.7 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.7)
Health Hazard Assessment (HHA)	FAA SSH, Chapter 8 NAS SSMP, Section 5.2.8 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.8)
System Safety Assessment Report (SSAR)	NAS SSMP, Section 5.2.9 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.9)
Safety Requirements Verification Table (SRVT)	NAS SSMP, Section 5.2.11 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.11)
Hazard Tracking System	FAA SSH, Section 2.2.3

System Safety Process Products	How To Reference
Hazard Tracking System (HTS)	NAS SSMP, Section 5.2.10 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.10)

4.8.2 Reliability, Maintainability, and Availability

4.8.3 Human Factors Engineering

4.8.4 Electromagnetic Environmental Effects

4.8.5 Quality Engineering — Reserved

4.8.6 Information Security Engineering

4.8.7 Hazardous Materials Management/Environmental Engineering

4.8.2 Reliability, Maintainability, and Availability Engineering

This section guides system engineers in facilitating and managing coordination of RMA efforts, which ensure operationally acceptable RMA characteristics in fielded systems.

4.8.2.1 What Is Reliability, Maintainability, and Availability Engineering?

Simply defined:

- *Reliability* quantifies a system's ability to perform without failure
- *Maintainability* quantifies a system's ability to recover from failure
- *Availability* quantifies a system's ability to perform when needed

RMA Engineering applies engineering and management principles, criteria, and techniques to optimize the RMA performance of a system within the program's operational and programmatic constraints. These engineering and related management tools are used to identify, evaluate, and control RMA characteristics associated with a system. Thus, the primary purpose of RMA Engineering is to minimize the probability of system failure and any potential losses stemming from such failure. RMA accomplishes this by establishing RMA requirements, assessing system RMA attributes, and analyzing solutions developed to meet established RMA requirements within realistic cost constraints.

4.8.2.1.1 Reliability, Maintainability, and Availability Detailed Definitions

These detailed RMA definitions provide background and context for the subsequent RMA Engineering discussions.

4.8.2.1.1.1 Reliability

Reliability is the probability that a system or constituent piece may perform a required function under specific conditions for a stated period of time. Reliability is calculated by the formula in Equation 1.

$$R = e^{-\frac{t}{m}}$$

Equation 1. Reliability Formula

where:

- *t is the mission time for which reliability is be calculated*
- *m is the mean-time-between-failure (MTBF),*
- *e is the natural antilogarithm of* $-\frac{t}{m}$.

MTBF is the basic measure of reliability for repairable systems or constituent pieces. MTBF is the mean number of life units during which all parts of the system or constituent pieces perform within their specified limits, during a particular measurement interval under stated conditions. MTBF is calculated according to Equation 2.

$$MTBF = \frac{T}{F}$$

Equation 2. MTBF Formula

where:

- *T is the length of the measurement interval*
- *F is the number of failures that occurred during the measurement interval*

4.8.2.1.1.2 Maintainability

Maintainability is the measure of the ability of a system or constituent piece to be retained in, or restored to, its fully operational status. It is generally characterized by the Mean-Time-To-Restore (MTTR), which is the total elapsed time from initial failure to resumption of operation. MTTR includes *all* "downtime"—not just the ease and speed with which a system may be repaired and returned to operational status following a failure. It is expressed as the sum of corrective diagnosis and maintenance times, divided by the total number of failures of a system or constituent piece Thus, the MTTR includes (and is thus greater than) the Mean-Time-To-Repair (see Equation 3). MTTR is usually expressed in hours.

$$MTTR = \sum_{t=1}^{F_T} \frac{\text{Diagnosis}_t + \text{Maintenance}_t}{F_T}$$

Equation 3. MTTR Formula

where:

- *t is an integer representing an occurrence requiring corrective diagnosis and associated corrective maintenance*
- *T is the length of the measurement interval*
- F_T *is the number of failures that occurred during the measurement interval*
- Diagnosis_t *is the time to perform corrective diagnosis*

- Maintenance_t *is the time to perform corrective maintenance*

Maintainability requirements generally pertain to inherent characteristics of the hardware design, such as the ability to isolate, access, and replace the failed component. These characteristics are generally fixed for commercial-off-the-shelf (COTS) components but may be specified, provided they do not conflict with the policy to employ COTS hardware whenever practical.

4.8.2.1.1.3 Availability

Availability is the probability that a system or constituent piece may be operational during any randomly selected instant of time or, alternatively, the fraction of the total available operating time that the system or constituent piece is operational. Measured as a probability, availability may be defined in several ways, which allows a variety of issues to be addressed appropriately, including:

- **Inherent Availability**. This availability is based solely on the MTBF and the MTTR characteristics of the system or constituent piece and the level of redundancy, if any, provided. For systems or constituent pieces employing redundant elements, perfect recovery is assumed. Downtime occurs only if multiple failures within a common timeframe result in outages of the system or one or more of its pieces to the extent that the need for redundant resources exceeds the level of redundancy provided. Inherent availability represents the maximum availability that the system or constituent piece is theoretically capable of achieving.

- **Equipment and Service Availability**. This availability includes all causes of unscheduled downtime (i.e., does not include scheduled downtime). This type of availability takes into account additional downtime incurred during the failover to redundant systems or downtime incurred by other practical issues associated with unscheduled outages.

- **Operational Availability**. This availability includes all sources of downtime, both scheduled and unscheduled.

The inherent availability represents the theoretical maximum availability that may be achieved by a system or constituent piece if automatic recovery is 100 percent effective. It strictly represents the theoretical availability based only on reliability (MTBF) and maintainability (MTTR). It does not include the effects of scheduled downtime, shortages of spares, unavailable service personnel, or poorly trained service personnel.

The availability requirement associated with the highest criticality service supplied by the system being procured is used to specify the inherent availability of the system. The only purpose for imposing an inherent availability requirement is to ensure that proposed constituent pieces of the system are *theoretically* capable of meeting a higher-level requirement, based on the reliability and maintainability characteristics of these constituent pieces and the redundancy provided.

Compliance with this requirement may be verified by using straightforward combinatorial availability models. The inherent availability of a single system or single constituent piece of the system is based on Equation 4.

$$A_{Single} = \frac{MTBF}{MTBF + MTTR}$$

Equation 4. Availability of a Single Element

Equation 5 gives the inherent availability of a string of system pieces that shall be up for the system to be operational.

$$A_{String} = A_1 A_2 A_3 \cdots A_n$$

Equation 5. Availability of a String of System Pieces

The right side of Equation 5 is the product of all terms in the sequence.

Figure 4.8-8 illustrates the inherent availability of a two-element system, which is considered operational if both elements are up—or if the first is up and the second is down, or if the first is down and the second is up (i.e., the system is available if either S1 or S2 is up and running)—and is expressed by Equation and Equation 7.

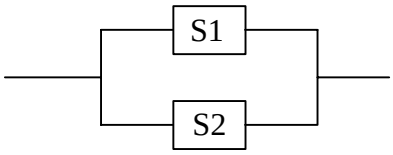


Figure 4.8-8. Inherent Availability of a Two-Element System

$$A_{Two-Element} = (A_1 A_2 + A_1 \overline{A}_2 + \overline{A}_1 A_2)$$

Equation 6. Availability of a Two-Element System

or

$$A_{Two-Element} = (1 - \overline{A}_1 \overline{A}_2)$$

Equation 7. Availability of a Two-Element System

where $\overline{A} = (1 - A)$ *, or the probability that an element is not available*

The above equations may be combined to model more complex architectures. However, it is recommended that the overriding goal for verifying compliance with the inherent availability requirement be *kept simple*.

4.8.2.2 Why Perform Reliability, Maintainability, and Availability Engineering?

Reliability, maintainability, and availability directly impact both operational capability and lifecycle costs and, therefore, are important considerations in any system engineering effort. A system's ability to successfully fulfill its mission need directly depends on its ability to perform its required function under specific conditions for a given period of time without failure (reliability). Likewise, a system's operational success also depends on its ability to recover from a failure in a timely and efficient manner (maintainability). Operational success also depends on the system being ready to accomplish its mission as needed (availability). It is widely recognized and accepted that a system's RMA characteristics directly impact its overall lifecycle costs. Operational and support costs for a system are predominant variables of its overall lifecycle cost. A major driver in operational and support costs is the quality of a system's RMA characteristics; thus, it is imperative that programs apply sound engineering and management principles, criteria, and techniques to ensure operationally acceptable RMA characteristics in fielded systems. As indicated in Equation 6, using redundancy is the simplest way to increase availability. When redundancy is used to increase system availability, the overall system lifecycle costs increases.

A system engineer—to effectively and successfully coordinate RMA Engineering efforts and, therefore, optimize the quality of a system's RMA characteristics—shall focus on the following RMA objectives, which are to be achieved throughout the lifecycle of a system:

- Identify all of the system's RMA functions, to include all operational and maintenance support drivers, in order to:
  - Comprehensively incorporate RMA principles into the system's requirements and design
  - Minimize and control the system's lifecycle costs
- Measure, predict, assess, and report system trends, throughout its lifecycle to continuously meet or exceed RMA performance requirements
- Achieve RMA performance objectives at all system levels
- Emphasize continuous RMA improvement

4.8.2.2.1 FAA Background on Reliability, Maintainability, and Availability

For the last 20 years, FAA specifications have focused primarily on availability requirements instead of the more traditional reliability and maintainability requirements.

Availability is appropriate as a top-level operational requirement because it is a quantitative and consistent way of summarizing the need for continuity of NAS services. Use of availability requirements may facilitate FAA system engineers' comparison and assessment of architectural alternatives. . Availability is also useful as a performance metric for operational systems.

However, using availability as the primary RMA requirement in contractual specifications presents many practical problems. The fundamental concept of availability seems to imply a tradeoff between reliability and maintainability. In other words, a 1-hour interruption of a critical service that occurs annually is apparently equivalent to 240 15-second interruptions of the same

service, since both scenarios provide the same availability. However, short interruptions lasting seconds are less likely to affect air traffic control operations than long interruptions lasting an hour or more, which may have a significant impact on traffic flow and operational safety.

In addition, availability cannot be measured during system development and may only be predicted by using highly artificial models. It is also impractical to measure the availability of a developed system before its operational deployment.

For these reasons, it is necessary to perform RMA Engineering to establish detailed RMA requirements that may be monitored and verified during development. Well-written RMA requirements ensure that the FAA understands what is to be received and that the supplier understands what shall be delivered.

4.8.2.2.2 Reliability, Maintainability, and Availability Policy

The Integrated Logistics Support (ILS) section of the FAA's AMS policy implies that the products of RMA Engineering are a fundamental key in achieving the ILS objective. ILS provides the required level of service to the end user at minimal lifecycle cost to the FAA. Thus, not only is it sound system engineering practice that drives programs to perform RMA Engineering (as stated in the sections above), but it is also a necessity to properly adhere to AMS policy.

4.8.2.3 Reliability, Maintainability, and Availability Inputs

Inputs to the RMA Engineering process include requirements, descriptions of alternatives, and functional architectures and physical architectures, as well as specific measurements and other data that may be used to analyze system performance in the interrelated RMA areas. (See Figure 4.8-1 for a list of possible inputs.) The inputs used within the RMA Engineering process shall be sufficient to enable computation of the two defining RMA characteristics (i.e., MTBF and MTTR) and comprehensive enough to conduct the appropriate analysis.

4.8.2.4 Reliability, Maintainability, and Availability Process Tasks

RMA Engineering follows the process tasks outlined in General Specialty Engineering Process Tasks (Paragraph 4.8.0.3).

4.8.2.5 Reliability, Maintainability, and Availability Outputs

Figure 4.8-1 lists the various outputs that may result from performing Specialty Engineering. The following subsections detail some of these outputs as they relate to RMA Engineering.

4.8.2.5.1 Planning Criteria

The application of an RMA program generally follows the steps described below. These steps shall be considered in providing planning criteria input to SE Integrated Technical Planning (Section 4.2).

4.8.2.5.1.1 STEP 1: Identify Desired RMA Program Objectives

This step includes identifying and documenting unambiguous and measurable objectives based on the mission need.

4.8.2.5.1.2 STEP 2: Select Metrics

Establishing metrics (see Paragraph 4.8.2.6) sets the stage for later evaluations. Metrics provide a level of program continuity in determining progress toward meeting RMA program objectives.

4.8.2.5.1.3 STEP 3: Establish Plans for Performance Monitoring

Monitoring plans shall be established and implemented early in the program. It is recommended that an RMA data system be incorporated early in the system's lifecycle to permit monitoring and assessment of RMA performance and to ensure that all RMA data recorded are appropriately disseminated, analyzed, and evaluated.

In conjunction with an effective RMA data system, it is recommended that a closed loop problem/failure reporting and corrective system be established to support problem detection, assessment, and correction. Such a system allows implementation of design improvements and corrections as part of the system development process as well as provides a tool for monitoring progress toward meeting system requirements, which obviously includes subset of the RMA requirements. The data collected supports tracking the root cause of the problem, which thus facilitates overcoming hurdles that may be hindering achievement of specific RMA requirements.

It is recommended that the corrective action system continue to be used during in-service operations to support upgrading system RMA performance in conjunction with a Reliability Growth Program (see Paragraph 4.8.2.5.1.3.1), if necessary. Operations truly demonstrate the system's actual capability to meet RMA requirements. Operations also provides a unique opportunity to continue evaluating and upgrading the system's RMA performance with the dual benefit of ensuring that the RMA performance meets and maintains intended capabilities and produces lower lifetime costs. It is recommended that the corrective action system developed and implemented early in the system's lifecycle continue to be used to support upgrading RMA performance.

Using a structured and controlled performance data acquisition process provides the information to perform trend analysis on the behavior of the system and to support root cause analysis. The application of RMA tools (see Paragraph 4.8.2.7) is extremely data-dependent and the root of oversight/insight into program behavior, validation decisions made earlier during initiation, and identification of modifications/actions to sustain the program. For example, if Reliability Centered Maintenance were incorporated early in the system's lifecycle, operations would provide the opportunity to validate or revise the maintenance decisions that were previously made during design. The most essential ingredient that helps guarantee the success of any RMA program is management's continuing commitment and support.

4.8.2.5.1.3.1 Reliability Growth Program

A Reliability Growth Program is usually necessary because a formal reliability demonstration test, in which the system is either accepted or rejected based on the test results, is not feasible. For a formal reliability demonstration, the test time required to obtain a statistically valid sample would be prohibitive, and the large number of software failures encountered in any major software development program would virtually ensure failure to demonstrate compliance with the requirements. Establishing "pass-fail" criteria for a major system acquisition is not a viable alternative.

Reliability growth testing is an ongoing process of testing, and correcting failures. Reliability growth was initially developed to discover and correct hardware design defects. Statistical methods were developed to predict the system MTBF at any point in time and to estimate the additional test time required to achieve a given MTBF goal.

Reliability growth testing applied to automation systems is a process of exposing and correcting latent software defects. The hundreds of software defects exposed during system testing, coupled with the stringent reliability requirements for these systems, preclude using statistical methods to accurately predict the test time to reach a given MTBF before system deployment. There is no statistically valid way to verify compliance with reliability requirements at the FAA's William J. Hughes Technical Center (WJHTC) before field deployment. This is because it is not possible to obtain enough operating hours at the WJHTC to reduce the number of latent defects to the level needed to meet the reliability requirements.

The inescapable conclusion is that it may be necessary to field systems that lack RMA requirements verification. The large number of additional operating hours accumulated by multiple system installations may increase the rate at which software errors are found and corrected, as well as the growth of the system MTBF.

To be successful, the reliability growth program shall address two issues. First, the contractor shall be aggressive in promptly correcting software defects. The contractor shall be given a powerful incentive to keep the best people on the job through its completion, instead of moving them to work on new opportunities. In the Host program, for example, a process called "expunging" accomplished this. The system MTBF was computed by dividing the operating hours by the number of failures. However, if the contractor demonstrated that the cause of the failure had been corrected, and then the failure was "expunged" from the list of failures. If a failure is not repeated within 30 days, it is also expunged from the database. Thus, if all Program Trouble Reports (PTRs) were fixed immediately, the computed MTBF would be infinite even if the system were failing daily.

This measure is statistically meaningless as a true indicator of the system MTBF. It is, however, a useful metric for assessing the responsiveness of the contractor in fixing the backlog of accumulated PTRs. Since government representatives decide when to expunge errors from the database, they have considerable leverage over the contractor by controlling the value of the MTBF reported to senior program management officials. There may be other or better metrics that could be used to measure the contractor's responsiveness in fixing PTRs; the important thing is that there shall be a process in place to measure the success of the contractor's support of reliability growth.

The second issue that shall be addressed during the reliability growth program is the acceptability of the system to field personnel. Since the system may be deployed to field sites before it has met the reliability requirements, it is recommended that field personnel be involved in the reliability growth testing at the WJHTC and concur in deciding when the system is sufficiently stable to warrant sending it to the field.

4.8.2.5.1.4 STEP 4: Report Results

Results of the performance-monitoring effort are reported to support assessment of the progress toward meeting requirements and meeting RMA program objectives. This includes comparing predicted and demonstrated RMA versus requirements and evaluating system RMA demand throughout the system's operational life.

4.8.2.5.1.5 STEP 5: Use Results for Planning, Managing, and Budgeting

Assessing progress toward meeting requirements and meeting RMA program objectives provides the feedback needed to adjust program planning, managing, and budgeting. The results may also be used to support related analyses, such as safety and logistics, and in emphasizing improvements in succeeding systems.

4.8.2.5.2 Design Analysis Reports

There are various types of RMA analyses conducted and eventually documented within a Design Analysis Report. A discussion of some of the more common RMA-related analyses follows.

4.8.2.5.2.1 Failure Modes and Effects Analysis

FMEA is an evaluation process for analyzing and assessing the potential failures in a system. The objective is to determine the effect of failures on system operation, identify the failures critical to operational success and personnel safety, and assess each potential failure according to the effects on other portions of the system. In general, these objectives are accomplished by itemizing and evaluating system composition and functions.

This type of analysis is a systematic method of identifying the failure modes of a system, constituent piece, or function and determining the effects on the next higher level of the design. The detection method (if any) for each failure mode may also be determined. An FMEA may be a quantitative or qualitative analysis and may be performed on all types of systems (e.g., electrical, electronic, or mechanical). If a quantitative FMEA is being performed, a failure rate is determined for each failure mode. The results of an FMEA may be used to generate the Failure Modes and Effects Summary (FMES), Figure 4.8-10, and are normally used to support the other analysis techniques of the System Safety Assessment (SSA) process, such as Fault Tree Analysis (FTA), Dependence Diagram (DD), or Markov Analysis (MA). Combinations of failures are not usually considered as part of the FMEA.

An FMEA is performed at a given level (system, subsystem, element, etc.) by postulating the ways the chosen level's specific implementation may fail. The effect of each failure mode is determined at the given level and usually the next higher level for each operating mode of the equipment. Sometimes, an FMEA may be focused toward a specific operating scenario as required to support a top-down FTA, DD, or MA.

The FMEA shall account for all safety-related effects and any other effects identified by the requirements. In cases where it is not possible to identify the specific nature of a failure mode, the worst-case effect shall be assured. If the worst case is unacceptable for the fault tree, the failure modes shall be examined at the next lower level. That is, if the FMEA is being conducted at the functional level, drop to the piece-part level and exclude components with no effect on the event under consideration. If the analysis is being conducted at a piece-part level, drop to consider specific failure mechanisms within the part. Another option is to redesign to improve redundancy or add monitoring.

Regardless of the level to which the FMEA is to be performed, the major steps of an FMEA include preparation, analysis, and documentation.

4.8.2.5.2.1.1 FMEA Preparation

Preparing an FMEA includes determining the FAA's requirements, obtaining current documentation, and understanding the operation of the function. It is important to know the FAA's expectations and requirements for the FMEA before beginning. If the FMEA requirements are not known, the FMEA may not meet the needs of the requester and may have to be redone.

FMEA requirements usually originate from a Preliminary Hazard Analysis activity such as an FTA, DD, or MA. The analyst needs to know the analysis level (functional versus piece-part), safety-related effects, other failure effects, and operational modes of interest. An FMEA is used to support the safety assessment process by providing failure rates to quantify the basic events of the FTA, DD, or MA. An FMEA may also be used to support verification of the FTA by comparing the FMEA failure modes with the basic events of the fault tree.

The final step before beginning to perform the analysis is to obtain the following information, which may be necessary to complete the analysis, or which may simplify the analysis activity:

- FMEA requirements, including safety-related and requested failure effects and specific operating modes of interest
- Specifications
- Current drawings and schematics
- Parts lists for each system or constituent piece
- Functional block diagrams
- Explanatory materials, including the theory of operation
- An applicable list of failure rates
- The FMEA on the previous generation or similar function
- Any design changes and revisions that have not yet been included on the schematic (**Note:** Designs may change frequently, and having the most up-to-date material reduces FMEA updates.)
- Preliminary list of component failure modes from previous FMEA, if applicable

  (**Note:** For FMEA performed early in the design stage, some of the above information may not be available, and assumptions or estimates may have to be made. Detailed documentation of these assumptions shall be maintained for traceability and to simplify future updates.)

4.8.2.5.2.1.2 Performing the Analysis

The analyst needs to review and understand the information gathered during preparation stage previously described. The analyst may also find it useful to understand the functions that the design being analyzed performs within the next higher level. After gaining sufficient knowledge,

the analyst identifies failure modes. Every feasible hardware failure mode is postulated at the level of the design being analyzed. Consideration is given to failure modes of the components or functions that make up the given level. Information to aid in determining the failure modes of the functions or components is provided in functional FMEA and piece-part FMEA (see Paragraphs 4.8.2.5.2.1.2.1 and 4.8.2.5.2.1.2.2).

Every identified failure mode is analyzed to determine its effect on the given level and usually on higher levels as well. Failure-effect categories are created for each different type of effect, and a code may be assigned to each effect category. Defining these codes simplifies the FMEA worksheet Figure 4.8-9 by moving the description of each effect from the worksheet to the body of the report. The FMEA worksheet provides a list of failure modes, effects, and rates. Each effect category shall have only one higher-level effect; otherwise, the effect categories need to be defined in more detail. For example, if the effect category is originally defined as "causes signal xyz to be out of specification," but an out of specification high condition causes a different effect from an out of specification low condition, then the effect category may be split to "…out of specification high" and "…out of specification low." Similarly, if the failure mode is found to cause two higher-level effects (e.g., "Loss of signal A" and "Loss of signal B"), then these two need to be combined to form a new effect category, "Loss of both signal A and B."

The means by which the failure is detected is usually determined and documented within the FMEA worksheets. Examples of detection methods include detection by hardware or software monitors, power-up tests, and maintenance checks.

For a quantitative FMEA, a failure rate is assigned to each failure mode. It is recommended that whenever possible, failure rates be determined from failure data or similar equipment already in field use. Industry sources of failure rates (including MIL-HDBK-217, MIL-HDBK-338, RAC "Nonelectronic Parts Reliability Data" (NPRD), and GIPED (Government Industry Data Exchange Program), MIL-HDBK-978, and Rome Laboratory's "Reliability Engineer's Toolkit") may also be used. The total failure rate for each failure effect category may be detailed in a summary sheet or summarized in the FMES.

There are two basic types of FMEAs: functional and piece-part. Functional FMEAs are typically performed to support the safety analysis effort; piece-part FMEAs are performed as necessary to provide further refinement of the failure rate. Piece-part FMEAs are typically done when the more conservative failure rates from a functional FMEA prevent the system or constituent piece from meeting the FTA probability of failure budget. A piece-part FMEA may also be useful for systems that rely on redundancy, since a functional FMEA may not reveal single component failures affecting more than one redundant element. Piece-part FMEAs are also useful for safety analysis of mechanical items and assemblies.

4.8.2.5.2.1.2.1 Functional FMEA

A functional FMEA may be performed at any indenture level. The appropriate level of subdivision is determined by the complexity of the system and the objectives of the analysis. If the required analysis is on a section of circuitry or mechanical devices larger than a particular function, it is recommended that it be broken down into functional blocks. This may mean defining each replaceable unit or item into many blocks. The FMEA task is simplified in each block and has as few outputs as possible. Once the functional blocks have been determined, a functional block diagram is to be created and each block labeled with its functional name. For each functional block, it is recommended that internal and interface functions are analyzed relative to system operation.

The next step is postulating the failure modes for each functional block. Determine the failure modes by thinking about the intent of the functional block and trying to determine how that function might fall regardless of the specific parts used. The analyst shall know the operation of the functional block well enough to be positive that no significant failure modes have been overlooked, including single component failures that could affect more than one redundant functional block. Given a clear description of the block's function, analysts often find many of the failure modes to be apparent.

Following is a simple example of functional failure modes:

The power supply circuitry that generates the 5 volts may be called a functional block. Some examples of functional failure modes include:

- Loss of 5 volts
- Voltage less than 5 volts
- Voltage greater than 5 volts
- Noise on 5 volts
- Short-to-ground or other voltage

There may be other failure modes based on circuit implementation.

The effect of each failure mode is determined by considering how the function fits into the overall design. Failure-effect categories are generally created for each effect type, and a failure-effect category code is assigned. All failure modes that cause this identical effect are assigned to the effect category. The effect category code may then be entered into the FMEA worksheet for each failure. Software and fault monitoring shall be considered when failure effects and means of detection are determined. As part of this analysis, the analyst shall also verify that the monitoring is able to detect the failure mode. To properly perform this analysis, the analyst shall have detailed knowledge of the system requirements and software design, including internal fault management techniques as applicable.

If a quantitative analysis is being performed, a failure rate is assigned to each failure mode. One technique is to perform a failure rate prediction for each block and apportion the failure rate across the various failure modes based on past experience of similar functions or other sources, allowing determination of probability of occurrence.

The analyst records the functional FMEA results in the worksheet. The example below may be modified to meet program needs. Different requirements may result in addition or deletion of some of the information. The analyst needs to ensure that the FMEA form and content meet the specific needs of the requester before beginning the analysis.

As the analysis progresses, it is recommended that the analyst informally record the following information for future FMEA maintenance and to assist in resolving FMEA questions.

- Justification of each failure mode
- Rationale for the assigned failure rate

- Rationale assigning a particular failure-to-a-failure effect category
- Documentation of any assumptions made

This documentation is usually not included in the FMEA report, but is retained for reference.

4.8.2.5.2.1.2.2 Piece-Part FMEA

A piece-part FMEA is similar to a functional FMEA, except that instead of analyzing at the functional or block diagram level, analysts assess the failure modes of each individual component contained in the item or function. A piece-part FMEA may be used to determine the failure effects of potential electrical, electronic, or mechanical failures. For example, the effect of failures of a resistor or motor shaft may be considered as part of a piece-part FMEA. Piece-part FMEAs on electronic equipment are usually performed only as necessary, when the more conservative results of a functional FMEA may not allow the item to meet the FTA probability of failure budget. This is due in part to the difficulty in determining the failure modes for complex components.

The first step in a piece-part FMEA is to create a list of all components to be covered by the FMEA. The next step is to determine the failure modes of each component type. This is the most difficult part of the piece-part FMEA, particularly FMEAs performed on electronic items containing complex integrated circuits. Determining all the failure modes of any but the simplest components, where industry data is available, is extremely difficult and sometimes impossible. When in doubt, make the worst-case assumptions of part failure modes.

462

463

Failure Modes and Effects Analysis (FMEA)							
System:					FMEA Description:		Date:
Subsystem of Unit:							Sheet_____ of _____
Component:					FTA or DD References:		File No.:
					Prepared by:		Revision:
Function Names	Function Code	Failure Mode	Mode Failure Rate	Failure Phase	Failure Effect	Detection Method	Comments

464 **Figure 4.8-9. Functional FMEA Worksheet**

465

Failure Modes and Effects Summary (FMES)									
Project No.:				FMES No.:			Date:		
Contract No.:				Supplier:			Sheet_____ of _____		
System:				Suppliers Part No.:			Revision:		
Subsystem of Unit:				Suppliers Dwg. Ref.:			Prepared by:		
Ref.	Failure Mode	Failure Rate	Phase	Effects on System	Symptoms 1) Controllers 2) Ground Crew 3) Maintenance	1) Causal Failure 2) Remarks	Causal Failure Ref.	Check Ref.	Failure Condition Ref.

Figure 4.8-10. Functional FMES Worksheet

4.8.2.5.2.2 Failure Modes and Effects Criticality Analysis

FMECA identifies potential design weaknesses through a systematic analysis approach. The approach considers all possible ways in which a component may fail (the modes of failure); the possible causes for each failure; the likely frequency of occurrence; the criticality of failure; the effects of each failure on systems operation (and on various system components); and any corrective action that may be initiated to prevent (or reduce the probability of) the potential problem from occurring in the future.

Essentially, an FMECA is generated from an FMEA by adding a criticality figure of merit. More information on performing an FMECA appears in Section 9.7 of the FAA's System Safety Handbook.

4.8.2.5.2.3 Fault Tree Analysis

Details on FTA contents and the steps involved in performing an FTA appear in Section 9.3 of the FAA's System Safety Handbook.

4.8.2.5.3 Requirements

The following subsections provide general guidelines in developing candidate RMA requirements that may arise as a result of RMA Engineering analysis efforts.

4.8.2.5.3.1 Reliability, Maintainability, and Availability Requirements

For systems that are to become direct replacements of existing systems, it is recommended that the RMA Engineering practitioner do the following:

- Locate the system being replaced within the higher-level architecture
- Identify the service thread or threads that the system supports
- Determine the criticality level of the service thread; if more than one service thread is supported, use the service thread with the highest criticality level
- Use the availability associated with the service thread with the highest criticality level as the basis for the system-level availability requirement

For systems that are not to become replacements of existing systems, it is recommended that the RMA Engineering practitioner do the following:

- Identify the criticality of the system according to the provided requirements
- Ensure that the requirements are consistent with the higher-level requirements and the associated NAS Architecture implementation plan being addressed

The primary objectives to be achieved in preparing the RMA provisions for a procurement package are as follows:

- Provide the specifications, including a system-level specification, defining the RMA requirements for the delivered system
- Define the effort required to provide the necessary documentation, engineering, and testing required to support monitoring of the design and development effort, risk management, design validation, and reliability growth testing activities
- Provide guidance concerning the design and data required to facilitate the technical evaluation of fault-tolerant design approaches, as well as programs for risk management, software fault avoidance, and reliability growth

The system-level specification serves as the basis for defining the design characteristics and performance that are expected of the system. From the standpoint of RMA characteristics, it is necessary to define the quantitative RMA and performance characteristics of the automatic fault detection and recovery mechanisms. It is also necessary to define the operational requirements

needed to permit FAA facilities personnel to perform real-time monitoring and control and manual recovery operations as well as diagnostic and support activities.

4.8.2.5.3.2 Monitor and Control Requirements

In addition to the requirements directly related to RMA, there are complementary requirements in the area of Monitor and Control (M&C). The requirements are complementary because M&C capabilities deal with functions related to monitoring and controlling RMA performance. These capabilities include such functions as the ability to monitor the status of system hardware and software; run diagnostics; reconfigure system hardware and software; and download software releases. M&C requirements are typically either local to the system site location or remotely away from the system site location. Types of M&C requirements include:

- **System Monitoring.** The critical user requirements for system monitoring are the number of parameters and events that need to be monitored and the allowable latency between the time an event occurs and the time that it is reported at the M&C console. These requirements determine design parameters, such as the frequency of polling of remote devices or the periodicity of their reporting. The number of parameters to be monitored and the frequency of reporting impose a steady-state communications and processing load on the system. A requirement for immediate notification of status changes or failures may cause excessive peak loads that may overwhelm the monitor and control processor.

- **System Control**. The primary system control requirement concerns the types of commands to be provided and the time between entering and executing a command.

- **M&C Computer-Human Interface.** Specifying the M&C Computer-Human Interface (CHI) requirements is a particularly challenging task. General statements such as “an effective user interface must be provided” only creates controversy over what constitutes “effective.” Attempts to provide detailed requirements for the CHI may stifle innovation or rule out COTS solutions; but if detailed specifications are not provided, there is a risk that the design may be deemed unacceptable. Both the RMA Engineering process and the Human Factors Engineering process (Section 4.8.3) are involved in defining M&C CHI requirements.

- **System Data Recording.** Data-recording requirements concern the number and types of data to be recorded and the sampling rates. Some of the data to be recorded may be error reports and status changes that occur asynchronously. Data-recording issues are similar to those for system monitoring. The requirements drive steady-state processing and communications overhead, and peak traffic from asynchronous events may overload the system.

  Estimating the load imposed by system recording is complicated by the fact that FAA systems typically allow selection of the data items to be recorded (e.g., for monitoring normal operations or for diagnosing specific problems). Unless specific recording scenarios are provided, the data-recording load may be indeterminate.

- **Data Reduction and Analysis.** These requirements apply to the offline analysis capabilities that are provided to process recorded data. The analysis capabilities to be provided depend on the characteristics of the specified system.

- **Startup/Startover**. These requirements apply primarily to computer systems. Since most computer systems being acquired are based on COTS hardware, these requirements are likely to be closely tied to the characteristics of the selected hardware and operating system.

- **Software Loading and Cutover**. These requirements concern the methods for obtaining a new version of software (either electronically or on some form of media); loading the new software into the machines; and cutting over to the new software version. These requirements also greatly depend on the specific system design.

- **Certification**. Certification requirements relate to both offline capabilities for verifying that an individual subsystem has been restored to operation and to online capabilities for verifying that an entire system is continuing to operate satisfactorily.

- **Transition**. Transition requirements define the temporary capabilities that allow transition safely from an existing system to a new system and reversion quickly to the old system if problems occur with the new system. The transition capabilities allow new systems to be safely introduced into a 24/7 environment. Transition requirements are typically for temporary switching systems that are removed once the new system has proven to be reliable.

- **Training Systems**. Training requirements refer to requirements for any separate equipment and systems that are needed for training, as well as the capability to partition the system so that the part used for training activities is isolated from the operational system.

4.8.2.6 Reliability, Maintainability, and Availability Metrics

At a minimum, RMA metrics are based on the system's MTBF (i.e., reliability), MTTR (i.e., maintainability), and availability (see Paragraphs 4.8.2.1.1 and 4.8.2.5.1.2 for further details).

4.8.2.7 Reliability, Maintainability, and Availability Tools

The following tables list the RMA tools.

4.8.2.7.1 Reliability Analysis Tools

Table 4.8-7. Reliability Analysis Tools

Activity	What Is Done	Why It Is Done	When It Is Called For	When It Is Performed
Alert Reporting	Document significant problem and nonconforming item data for exchange between the FAA and GIDEP.	Identifies potential problems.	Used throughout a program (extends beyond just RMA).	As close to problem identification as possible.

Activity	What Is Done	Why It Is Done	When It Is Called For	When It Is Performed
Human Error Risk Assessment	Identify risks to design, equipment, procedures, and tasks as a result of human error.	Identifies candidate designs to support both risk and maintainability goals.	Appropriate for all programs.	Initially early in design and iteratively as the design matures.
Human Factors Task Analysis	Analyze and list all the things people may do in a system, procedure, or operation with details on: (a) information requirements; (b) evaluations and decisions that shall be made; (c) task times; (d) operator actions; and (e) environmental conditions.	Identifies influence factors that drive design for maintainability.	Appropriate for all programs.	Initially early in design and iteratively as the design matures.
Failure Mode and Effects (and Criticality) Analysis (FMEA/FMECA)	Perform a systematic analysis of the local and system effects of specific component failure modes. Under FMECA, also evaluate the mission criticality of each failure mode.	Identifies potential single failure points requiring corrective action. Identifies critical items and assesses system redundancy.	Recommended for consideration for all systems.	When a system block diagram is available. Update throughout system design.
Fault Tree Analysis (FTA)	Systematically identify all possible causes leading to system failure or an undesirable event or state	Permits systematic, top-down, penetration to significant failure mechanisms.	Apply to critical (especially safety-critical) systems.	During system design.
Problem/Fail	Provide a closed	Ensures that	All programs	Throughout

Activity	What Is Done	Why It Is Done	When It Is Called For	When It Is Performed
Pure Reporting and Corrective Action System (PRACA/ FRACAS)	loop system for documenting hardware and software anomalies, analyzing their impact on RMA, and tracking them to their resolution. (Root Cause Analysis)	problems are systematically evaluated, reported, and corrected.	may benefit from some type of formal, closed-loop system.	system lifecycle.
Problem/ Failure Reporting Plan	Document the process for closed-loop problem/failure identification, reporting, and resolution.	Shows what problems exist within the program, what has been done to correct them, and the effectiveness of the remedial action.	At the outset of a program.	Throughout system lifecycle.
Process Failure Modes and Effects Analysis	Analyze an operation/process to identify the kinds of errors that humans could make in carrying out the task.	Ensures a method to deduce the consequences for process failures and the probabilities of those consequences occurring.	To assist in the control of critical processes.	Early in process definition.
Reliability Assurance Plan	Identify the activities essential in ensuring reliable performance, including design, production, and product operation.	Ensures that design risks are balanced against program constraints and objectives through a comprehensive effort calculated to contribute to system reliability over the mission lifecycle.	For all programs with reliability performance requirements.	During program planning.
Reliability Modeling	Perform prediction, allocation, and	Aids in evaluating the reliability of competing designs.	Most hardware programs benefit where	Early in design.

Activity	What Is Done	Why It Is Done	When It Is Called For	When It Is Performed
(Prediction/ Allocation)	modeling tasks to identify inherent reliability characteristics.	competing designs.	failure rates are needed for tradeoff studies, sparing analysis, etc.	
Redundancy Switching Analysis	Perform a rigorous failure modes, effects, and criticality analysis (FMECA) at the part level for all interfacing circuits of redundant equipment.	Verifies that the failure of one of two redundant functions does not impair the ability to transfer to the second function.	Recommended for consideration for redundant equipment.	Early in design.
Reliability Tradeoff Studies	Compare all realistic alternative reliability design approaches against cost, risk, schedule, and performance impacts.	Aids in deriving the optimal set of reliability performance requirements, architecture, baselines, or designs.	Performed at some level on all systems. Predictive techniques may be used.	Investment Analysis and Solution Implementation.
Reliability Growth Test	Conduct repetitive test and repair cycles to disclose deficiencies and verify that corrective actions may prevent recurrence.	Provides gradual evolution of a system to a state of higher reliability through repeated failure and repair.	Appropriate for all hardware and software systems.	Beginning with design and throughout the product lifecycle.
Sneak Circuit Analysis	Methodically identify sneak conditions (unexpected paths or logic flows) in circuits.	Identifies design weaknesses that could inhibit desired functions ort initiate undesired functions.	Generally used only for the most safety-critical equipment.	Early in design.
Trend Analysis	Evaluate variation in data with the	Provides a means of assessing the	Used to track failures,	Throughout the

Activity	What Is Done	Why It Is Done	When It Is Called For	When It Is Performed
Analysis	ultimate objectives of forecasting future events based on examination of past results.	status of a program or the maturity of a system or equipment and predicting future performance.	anomalies, quality processes, delivery dates, etc.	program.

582

583 **4.8.2.7.2 Maintainability Analysis Tools**

584 **Table 4.8- 8. Maintainability Analysis Tools**

Activity	What Is Done	Why It Is Done	When It Is Called For	When It Is Performed
Link Analysis	Arrange the physical layout of instrument panels, control panels, workstations, or work areas to meet specific objectives (e.g., increased accessibility).	Provides as assessment of the connection between (a) a person and a machine or part of a machine; (b) two persons; or (c) two parts of a machine.	During design for maintainability.	During Mission Analysis and Investment Analysis.
Maintainability Modeling (Prediction/ Allocation)	Perform prediction, allocation, and modeling tasks to estimate the system mean-time-to-restore requirements.	Determines the potential of a given design for meeting system maintainability performance requirements.	Whenever maintainability requirements are designated in the design specification.	Early in Solution Implementation.
Maintenance Concept	Describe what, how, and where preventive and corrective maintenance is to be performed.	Establishes the overall approach to maintenance for meeting the operational requirements and the logistics and maintenance objectives.	Performed for any system where maintenance is a consideration.	During Mission Analysis and revise throughout the lifecycle.
Maintenance	Describe the	Provides the basis	A Maintenance	Begins

Activity	What Is Done	Why It Is Done	When It Is Called For	When It Is Performed
Engineering Analysis	planned general scheme for maintenance and support of an item in the operational environment.	for design, layout and packaging of the system and its test equipment and establishes the scope of maintenance resources required to maintain the system.	Plan may be substituted on smaller programs in which maintainability prediction and analysis are not required.	during design and iterated through develoment.
Maintenance Plan	Detail how the support program is to be conducted to accomplish the program goals.	Identifies the desired long-term maintenance characteristics of the system and the steps for attaining them.	Appropriate for all hardware programs.	Prepare during Investment Analysis and update throughout the life of program.
Reliability Centered Maintenance (RCM)	Determine the mix of reactive, preventive, and proactive maintenance practices to provide the required reliability at the minimum cost.	Minimizes or eliminates more costly unscheduled maintenance and minimizes preventive maintenance.	Appropriate for all hardware programs. Generally called for as part of the maintenance concept.	During Solution Implementation.
Testability Analysis	Assess the inherent fault detection and failure isolation characteristics of the equipment.	Improves maintainability in response to operational requirements for quicker response time and increased accuracy.	Applicable to all hardware systems; however, especially appropriate where maintenance resources are available but restrained.	Early in design.
Tradeoff Studies	Compare realistic alternative maintainability design approaches	Determines the preferred support system or maintenance approach in	Performed where alternate support approaches or	Complete early in the acquisition cycle (see Section

Activity	What Is Done	Why It Is Done	When It Is Called For	When It Is Performed
	against cost, schedule, risk, and performance impacts.	accordance with risk, performance, and readiness objectives.	maintenance concepts involve high-risk variables.	4.6).

4.8.2.8 References

1. Aerospace Recommended Practice, ARP4761 “Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.” Issued 1996-12. Society of Automotive Engineers, Inc.

2. “Guide to the Assessment of Reliability" 89/97714—Guide to the Assessment of Reliability of Systems Containing Software," British Standards Institution, 12 September 1989.

3. “System Safety Handbook,” Federal Aviation Administration, 30 September 2000.

4.8.3 Human Factors Engineering

4.8.3.1 What Is Human Factors Engineering?

Human factors engineering is a multifaceted discipline that generates information about human requirements and capabilities and applies it to the design and acquisition of complex systems (see Figure 4.8-11). Human factors engineering provides the opportunity to: (1) develop or improve all human interfaces with the system; (2) optimize human/product performance during system operation, maintenance, and support; and (3) make economical decisions on personnel resources, skills, training, and costs. Embedding and integrating human factors engineering activities into the acquisition of systems and equipment lower lifecycle costs, improves overall performance, and reduces technical risk. Failure to apply the disciplines of human factors engineering has consistently resulted in development of systems that do not satisfy the needs of the workforce and often result in costly delays and extensive rework.

Human factors engineering is a multidisciplinary effort to generate and compile information about human capabilities and limitations and apply that information to:

- **Equipment, Systems, Software, Facilities**
- **Procedures, Jobs, Organizational Design, Environments**
- **Training, Staffing, Personnel management**

To produce safe, comfortable, and effective human performance.

Figure 4.8-11. Definition of Human Factors Engineering

4.8.3.2 Why Perform Human Factors Engineering?

Experience has proven that when people think of acquiring a system, they tend to focus on the hardware and the software. Individuals often fail to visualize that people operate and maintain the hardware/software. These people have different aptitudes, abilities, and training and operate system under various operating conditions, organizational structures, procedures, equipment configurations, and work scenarios. The total composite of these elements and the human component determines the performance, safety, and efficiency of the system in the NAS. To produce an effective human factors engineering program for any acquisition, it is recommended that the definition of the system include not only the *hardware, software, facility, and services*, but also the *users* (*operators and maintainers)* and the *environment* in which the acquisition is used.

Applied early in the lifecycle acquisition management process, human factors engineering enhances the probability of increased performance, safety, and productivity; decreases lifecycle staffing and training costs; and becomes well-integrated into the program's strategy, planning, cost and schedule baselines, and technical tradeoffs. Changes in operational, maintenance, or design concepts during the later phases of an acquisition are expensive and entail high-risk program adjustments. Identifying lifecycle costs and human performance components of

system operation and maintenance during investment analysis and requirements definition decreases program risks and long-term operations costs. These benefits are applicable to COTS and non-developmental items (NDI) as well as to developmental programs.

4.8.3.3 Inputs to the Human Factors Engineering Process

The FAA Human Factors Job Aid guidelines are in the FAA Acquisition System Toolset (FAST). These guidelines contain extensive information regarding the integration of human factors engineering activities into the acquisition management process. It is recommended that IPTs be familiar with this information and embed human factors engineering principles into their acquisition programs. The Human Performance Interfaces in Systems Acquisition (Table 4.8-9) identify and define the many classes of human interfaces the IPT may need to consider as it plans and implements equipment/system acquisition programs. Analysis of these interfaces may provide a basis for determining the inputs to the human factors engineering process tasks. These inputs may include new or previously conducted human factors research, studies, and analyses; human factors standards and guidelines; human factors technical methods and techniques; human performance data criteria; or other human-system interaction information.

Table 4.8-9. Human Performance Interfaces in Systems Acquisition

Human Interface Class	Performance Dimension	Performance Objective
Functional Interfaces: For operations and maintenance - role of the human versus automation; functions and tasks; manning levels; skills and training	Task performance	Ability to perform tasks within time and accuracy constraints
Information Interfaces: Information media, electronic or hardcopy; information characteristics, and the information itself	Information handling/processing performance	Ability to identify, obtain, integrate, understand, interpret, apply, and disseminate information
Environmental Interfaces: Physical, psychological, and tactical environments	Performance under environmental stress	Ability to perform under adverse environmental stress, including heat and cold, vibration, clothing, illumination, reduced visibility, weather, constrained time, and psychological stress
Operational Interfaces: Procedures, job aids, embedded or organic training, and online help	Sustained performance	Ability to maintain performance over time

Human Interface Class	Performance Dimension	Performance Objective
Organizational Interfaces: Job design, policies, lines of authority, management structure, organizational infrastructure	Job performance	Ability to perform jobs, tasks, and functions within the management and organizational structure
Cooperation Interfaces: Communications, inter personal relations, team performance	Team performance	Ability to collectively achieve mission objectives
Cognitive Interfaces: Cognitive aspects of human-computer interfaces (HCI), situational awareness, decision-making, information integration, short-term memory	Cognitive performance	Ability to perform cognitive operations (e.g., problem-solving, decision making, information integration, situational awareness)
Physical Interfaces: Physical aspects of the system with which the human interacts (e.g., HCI, controls and displays, workstations, and facilities)	Operations and maintenance performance	Ability to perform operations and maintenance at workstations and worksites, and in facilities using controls, displays, equipment, tools, etc.

Addressing the human performance limitations and capabilities would seem to be a daunting task unless the task were divided into its many components and unless human factors is described in some descriptive taxonomy of issues. Thus, the potential human factors risks and areas of interest may be reflected as elements of the human factors issue areas listed in Table 4.8-10.

Table 4.8-10. Human Factors Issue Areas

Human Factors Issue Areas
1. **Allocation of Function** — System design reflecting assignment of those roles/functions/tasks for which the human performs better, or assignment to the equipment that it performs better while maintaining the human's awareness of the operational situation. 2. **Anthropometrics and Biomechanics** — System design accommodation of personnel (e.g., from the 1st through the 99th percentile levels of human physical characteristics) represented in the user population. 3. **Communications and Teamwork** — System design considerations to enhance required user communication and teamwork. 4. **Computer Human Interface (CHI)** — Standardization of CHI to access and use common functions employing similar and effective user dialogues, interfaces, and procedures.

58

Human Factors Issue Areas
5. **Displays and Controls** — Design and arrangement of displays and controls to be consistent with the operator's and maintainer's natural sequence of operational actions and provide easily understandable supporting information. 6. **Documentation** — Preparation of user documentation and technical manuals in a suitable format of information presentation, at the appropriate reading level, easily accessible, and with the required degree of technical sophistication and clarity. 7. **Environment** — Accommodation of environmental factors (including extremes) to which equipment is to be subjected and the effects of environmental factors on human-system performance. 8. **Functional Design and Operational Suitability** – Use of a human-centered design process to achieve usability objectives and compatibility of equipment design with operation and maintenance concepts and legacy systems. 9. **Human Error** — Examination of unsafe acts, contextual conditions, and supervisory and organization influences as causal factors contributing to degradation in human performance, and consideration of error tolerance, resistance, and recovery in system operation. 10. **Information Presentation** — Enhancement of operator and maintainer performance through use of effective and consistent labels, symbols, colors, terms, acronyms, abbreviations, formats, and data fields. 11. **Information Requirements** — Availability of information needed by the operator and maintainer for a specific task when it is needed and in the appropriate sequence. 12. **Input/Output Devices** — Design of input and output devices and methods that support performing a task quickly and accurately, especially critical tasks. 13. **Knowledge, Skills and Abilities (KSA)** — Measurement of the knowledge, skills, and abilities required to perform job-related tasks. Necessary to determine appropriate selection requirements for operators. 14. **Procedures** — Design of operational and maintenance procedures for simplicity and consistency with the desired human-system interface functions. 15. **Safety and Health** — Reduction/prevention of operator and maintainer exposure to safety and health hazards. 16. **Situation Awareness** — Consideration of the ability to detect, understand, and project the current and future operational situations. 17. **Skills and Tools** — Considerations to minimize the need for unique operator or maintainer skills, abilities, or characteristics. 18. **Staffing** — Accommodation of constraints and opportunities on staffing levels and organizational structures. 19. **Subjective Workload** — The operator's or maintainer's perceived effort involved in managing the operational situation. 20. **Task Load** — Objective determination of the numbers and types of tasks that an operator performs.

59
60

Human Factors Issue Areas
21. **Training** — Consideration of the acquisition and decay of operator and maintainer skills in the system design and capability to train users easily, and design of the training regimen to result in effective training. 22. **Visual/Auditory Alerts** — Design of visual and auditory alerts (including error messages) to invoke the necessary operator and maintainer response to adverse and emergency situations. 23. **Workspace** — Adequacy of workspace for personnel and their tools and equipment, and sufficient space for movements and actions they perform during operational and maintenance tasks under normal, adverse, and emergency conditions.

4.8.3.4 Human Factors Engineering Process

The process of integrating human factors engineering into acquisition programs entails numerous technical and management activities. Many of these activities are conducted iteratively through several phases of the acquisition and often in a nonlinear sequence. While the process flow is described below in 15 activities (listed in Table 4.8-11), other subordinate activities (e.g., critical task analysis, target audience analysis, cognitive analysis, human-in-the-loop simulation, and CHI prototyping) are also required. A description of these subordinate tasks are in the FAA Human Factors Job Aid or in more detailed human factors engineering reference manuals.

Table 4.8-11. Human Factors Engineering Process Activities

Human Factors Engineering Process Activities
1. Incorporate Human Factors Opportunities and Constraints into the MA and Mission Need Statement (MNS) 2. Incorporate Human Factors Requirements in Requirements Document 3. Incorporate Human Factors Assessment in the Investment Analysis 4. Incorporate Human Factors Parameters in the Acquisition Program Baseline (APB) 5. Designate Human Factors Coordinator for the PT 6. Establish Human Factor Working Group 7. Incorporate Human Factors Strategy into the ASP 8. Incorporate Human Factors Tasks into the IPP 9. Develop Integrated Human Factors Plan 10. Incorporate Human Factors Requirements into System Specifications and Statement of Work 11. Include Human Factors in Source Evaluation Criteria 12. Conduct Human Factors Engineering Analyses 13. Apply Human Factors Engineering to System Design 14. Test System Against Human Performance Requirements 15. Conduct In-Service Review for Human Factors

4.8.3.5 Human Factors Engineering Process Tasks

The following process flow provides an outline and overview of key activities in the human factors engineering process.

Activity 1: Incorporate Human Factors Opportunities and Constraints Into the Mission Analysis and Mission Need Statement			
Responsible Agent	**Product**	**Approval Authority**	**Tools and Aids**
Mission Analysis and MNS Sponsor	Human factors input on opportunities and constraints to the MNS	Mission Analysis Manager MNS Sponsor	Guidance on developing human factors input to the MA and MNS

Description:

Using the results from the mission analysis, human factors engineering inputs to the MNS identify the human performance constraints and issues that need to be addressed or resolved. This information may come from operations and maintenance concepts, similar systems or components, and other documents that may provide insights into the effects of human factors engineering constraints and limitations on system performance. Since most acquisitions are evolutionary, important human factors engineering information may be obtained from predecessor systems or their component subsystems. Analyses and tradeoff studies may be required to determine the effects of constraints and issues on system performance. It is recommended that the existing literature and lessons learned databases be reviewed.

Activity 2: Incorporate Human Factors Requirements in the RD			
Responsible Agent	**Product**	**Approval Authority**	**Tools and Aids**
Requirements Sponsor	Human factors requirements in the iRD or fRD	IRT Lead	Guidance on developing human factors requirements for the RD

Description:

The initial RD contains generic performance and supportability requirements that do not prescribe a specific solution. The RD defines the essential performance capabilities and characteristics, including those of the human component. Human factors engineering inputs to the RD identify requirements for human performance factors that impact system design. Broad cognitive, physical, and sensory requirements for the operator, maintainer, and support personnel that contribute to or constrain total system performance are established. It is recommended that any safety, health hazards, or critical errors that reduce job performance or system effectiveness be defined, and that staffing and training concepts, including requirements for training devices, embedded training, and training logistics, also be described.

Activity 3: Incorporate Human Factors Assessment in the Investment Analysis			
Responsible Agent	**Product**	**Approval Authority**	**Tools and Aids**
Investment Analysis Sponsor	Human factors input to the IA Plan Human Factors Assessment (including risk, cost, and benefits) for the IA	IAT Lead	Guidance on developing Human Factors Assessments for the IA

Description:

Human factors engineering inputs to the IAR address, for each alternative being evaluated, the full range of human performance and interfaces (e.g., cognitive, organizational, physical, functional, and environmental) necessary to achieve an acceptable level of performance for operating, maintaining, and supporting the system. It is recommended that the analysis provide information on what is known and unknown about human performance risks in meeting minimum system performance requirements. Human factors engineering areas of interest relevant to the investment analysis include:

- Human performance (e.g., human capabilities and limitations, workload, function allocation, hardware and software design, decision aids, environmental constraints, team versus individual performance)
- Training (e.g., length of training, training effectiveness, retraining, training devices and facilities, embedded training)
- Staffing (e.g., staffing levels, team composition, organizational structure)
- Personnel selection (e.g., aptitudes, minimum skill levels, special skills, experience levels)
- Safety and health hazards (e.g., hazardous materials or conditions, system or equipment safety design, operational or procedural constraints, biomedical influences, protective equipment, required warnings and alarms)

Activity 4: Incorporate Human Factors Parameters in the APB			
Responsible Agent	**Product**	**Approval Authority**	**Tools and Aids**
APB Sponsor	Human factors performance parameters in the APB	IAT Lead	Guidance on developing human factors parameters for the APB

Description:

The APB is established at the Investment Decision and reflects the solution selected by the JRC for implementation. Based on the solution selected, human factors engineering inputs to the APB are those human performance requirements needed to achieve the required level of system performance. These inputs are derived from those identified in the Requirements Document and reflect a refinement that provides increased definition, greater granularity, and more specificity of relevant human-system performance characteristics. It is recommended that constraints, limitations, and unique or specialized training requirements, staffing levels, or personnel skill requirements be identified.

It is recommended that, to the degree possible, the required level of human performance be based on practical measures of operational effectiveness and suitability and be stated in quantifiable terms (e.g., time to complete a given task, level of accuracy required, number of tracks to be processed per unit time).

Activity 5: Designate Human Factors Coordinator for the PT			
Responsible Agent	**Product**	**Approval Authority**	**Tools and Aids**
PT Leader	Human Factors Coordinator	System Engineer	Guidance on developing a human factors program

Description:

The Product Team Leader designates a Human Factors Coordinator to develop, direct, and monitor human factors engineering activities during system acquisition. It is recommended this designation occur as early as during Investment Analysis to ensure human considerations are an integral element of market surveys, tradeoff analyses, and the definition of requirements for candidate solutions to mission need. The Human Factors Coordinator:

- Defines human impacts and constraints during Investment Analysis and determination of requirements
- Evaluates human-system interfaces during market surveys, tradeoff analyses, and prototypes
- Prepares and updates human factors engineering portions of program planning documents, procurement packages, performance criteria and measures, and data collection efforts
- Develops and analyzes operational scenarios and human-system modeling for operators and maintainers
- Reviews and assesses human factors engineering concepts and designs
- Coordinates human factors engineering efforts and workgroup activities
- Coordinates human factors engineering with other disciplines

Activity 6: Establish Human Factor Working Group			
Responsible Agent	Product	Approval Authority	Tools and Aids
Human Factors Coordinator	Human factors Working Group	Systems Engineer	Guidance on human factors working groups

Description:

The Human Factors Coordinator may establish and chair a Human Factors Working Group (HFWG) to facilitate accomplishment of human factors engineering tasks and activities. The composition of the HFWG is tailored to the needs of the acquisition program. Membership typically consists of Product Team members, with outside members participating as needed.

Activity 7: Incorporate Human Factors Strategy Into the ASP			
Responsible Agent	Product	Approval Authority	Tools and Aids
PT systems engineering specialist with assistance from the Human Factors Working Group	Human factors strategy in the ASP	PT Lead	Guidance for developing HF strategy for the ASP

Description:

The human factors strategy depends on the size, cost, and complexity of the system to be acquired, as well as the nature and complexity of the human-product interface. It is recommended that the human factors engineering strategy address such factors as:

- Scope and level of human factors engineering required from the systems contractor
- Human factors engineering roles and responsibilities of organizations and contractors
- Means for evaluating the human-machine interface and achieving user buy-in
- Data sources and facilities needed
- Distribution of funding and resources
- Timing and scope of human factors engineering activities
- Relationship of human factors engineering with other program elements.

The HFWG may assist in developing strategies appropriate for different types of acquisition programs, such as those that procure NDIs, COTS products, or fully developed new systems.

Activity 8: Incorporate Human Factors Tasks Into the IPP			
Responsible Agent	Product	Approval Authority	Tools and Aids
PT systems engineering specialist with assistance from the Human Factors Working Group	Human factors tasks in the Integrated Program Plan	System Engineer	Guidelines for developing HF tasks for the IPP Human Factors Strategy Human Factors Requirements

Description:

The human factors section of the Integrated Program Plan defines the individual human factors engineering work tasks that shall be done during program implementation. For each task, the IPP assigns the responsible person and organization, identifies any output and the approval authority, specifies when the task is to be completed, and allocates resources. As the program progresses through Solution Implementation, the human factors section of the IPP is updated to reflect changes in program strategy or execution and to provide more planning detail as it is developed.

Activity 9: Develop Integrated Human Factors Plan			
Responsible Agent	Product	Approval Authority	Tools and Aids
Human Factors Coordinator	Integrated Human Factors Plan	PT Lead	Template for Integrated Human Factors Plan

Description:

For complex system acquisition programs, the Product Team may wish to prepare an Integrated Human Factors Plan. (See Table 4.8-12 for an outline of the content.) Tasks associated with this plan include:

- Defining the operational concept and support concept
- Describing the target population
- Defining human / system interfaces
- Defining human impacts of the system
- Defining the human factors engineering strategy
- Defining human factors engineering implementation activities

183 **Table 4.8-12. Integrated Human Factors Plan Content and Format**

Headings		Content
Background	Program Summary	• Briefly describe the program • Describe concept of operation and maintenance
	Program Schedule	• Provide overview of system acquisition schedule
	Target Population	Identify: • Operator and maintainer • Demographics • Biographical data • Previous training • Aptitudes • Task-related experience • Anthropometric data • Physical qualifications • Organizational relationships • Workspace requirements
	Guidance	• Summarize any guidance received
	Constraints	• State if additional staffing is required by the new system • State whether an existing job series is to be used or a new one created • Post limits on the amount of time that may be afforded for training • Establish standards on the working conditions that are to be acceptable when the new system is fielded • Describe limitations imposed by maintenance policy • Develop requirements as a result of union agreements
Issues and Enhancements	Issue Description	Describe the issue or problem background, importance, and consequences or task to be done to support the acquisition

Headings		Content
	Objectives	• Identify Human Factors Program objectives • Provide performance measures and criteria in terms of time and accuracy to perform tasks to evaluate resolution of issue • When human performance thresholds are known, identify tasks for the developer to be done early enough in the acquisition to influence requirements and system engineering • Identify the actions to be taken to resolve each issue • Show the current status of each issue
	Actions	• Identify actions to be taken to resolve issues • Show current status of each action
Activities	Activity Description	• Identify any tasks, studies, or analyses that shall be performed to resolve the issues (e.g., contractor's Human Engineering Program Plan per MIL-HDBK-46855, Functional Analysis to support equipment versus people allocation of functions, Task Analysis to produce a specific operator, and maintainer task list)
	Activity Schedule	• By acquisition phase, describe the human factors tasks in terms of who, what, when, and how (resources) • Identify feeds to and dependencies on ILS, training, and test and evaluation programs
Strategy	Goals and Requirements	• Derive Strategy from the major concerns, issues, schedule, tasks, guidance, constraints, objectives, and approach for the Human Factors Program • Answer the question, "What objectives does the government wish to achieve?" • Answer the question, "How is the government to accomplish these objectives?"
	Approach	• Identify who is to be responsible for the Human Factors Program • Set out the extent of contractor support required • Define how human factors resources are to be organized and managed to support the system acquisition

Headings		Content
	References	• Identify relevant references needed for a full understanding of the Human Factors Program
Review	Review	• Identify administrative handling procedures • Identify update schedule and procedure • Identify review procedures

184

Activity 10: Incorporate Human Factors Requirements Into System Specification and Statement of Work			
Responsible Agent	Product	Approval Authority	Tools and Aids
PT systems engineering specialist and human factors specialist	- Human factors requirements in the System Specification - Human Factors tasking in the Statement of Work - Human Factors data items in the Contractor Deliverable Requirements List (CDRL) - Human Factors data item descriptions	PT Lead	- Guidance on formulating human factors requirements in the System Specification - Guidance on defining human factors tasking in the Statement of Work - Data Item Descriptions for human factors

185 **Description:**

186 The System Specification and Statement of Work are the mechanisms for translating human
187 performance requirements and appropriate human factors engineering work tasks to the
188 contractor in a clear, unambiguous, and contractually binding document. The System
189 Specification addresses the following elements to ensure that required human performance
190 influences system design effectively:

191 • staffing constraints

192 • required operator and maintainer skills

193 • training time and cost for formal, informal, and on-the-job skill development

- acceptable levels of human and system performance when operated and maintained by the training population.

The Statement of Work shall contain all human factors tasking to be imposed on the contractor, as well as define data deliverables in the CDRL and associated Data Item Descriptions (DID).

Activity 11: Include Human Factors in Source Evaluation Criteria			
Responsible Agent	Product	Approval Authority	Tools and Aids
PT systems engineering specialist with assistance from the Human Factors Working Group	Human factors source evaluation criteria	PT Lead	Guidance for specifying human factors in source selection

Description:

It is recommended that human performance be a candidate as a major evaluation factor in source selection. By providing vendors a clear indication that the government attributes significant weight to how operators and maintainers perform with the system, the agency sends a strong message that operational suitability and effectiveness are of utmost importance.

Activity 12: Conduct Human Factors Engineering Analyses			
Responsible Agent	Product	Approval Authority	Tools and Aids
Contractor (or other performing agent) conducts analyses	Appropriate data as specified in the CDRL and DIDs (or other designated documentation)	Appropriate official as designated in the CDRL (or other designated documentation)	Human Factors Design Standard Human Factors Data Item Descriptions

Description:

The Product Team oversees, monitors, and reviews human factors engineering analyses conducted by the system contractor or other performing agent. These analyses may involve:

- Defining and allocating system functions
- Analyzing information flow and processing
- Estimating operator and maintainer capabilities
- Defining and analyzing tasks and workloads

Activity 13: Apply Human Factors Engineering to System Design			
Responsible Agent	Product	Approval Authority	Tools and Aids
Contractor designs system PT Human Factors Coordinator oversees and reviews	Integration of Human factors requirements into system design	System Engineer	Guidance for integrating human factors during detailed design

Description:

Human factors engineering is applied to system design activities to optimize human-system interfaces and ensure that human performance requirements are satisfied. Human factors engineering is applied to the full scope of system design, including experiments, tests, and studies; engineering drawings; work environment, crew station, and facility design; performance and design specifications; procedure development; software development; and manuals. The following are used effectively in defining human-product interfaces during system design:

- Prototypes and computer models
- Three-dimensional mockups
- Scale models
- Dynamic simulation

Activity 14: Test System Against Human Performance Requirements			
Responsible Agent	Product	Approval Authority	Tools and Aids
Contractor and government conduct testing PT Human Factors Specialist oversees and evaluates	Test results on human performance requirements	System Engineer System Test Official	Guidance on human factors engineering activities during test and evaluation

Description:

Compliance of the system with human performance requirements is tested as early as possible in system development. Human factors engineering findings from design reviews, prototype reviews, mockup inspections, demonstrations, and other early engineering tests are used in planning and conducting later tests. Human factors engineering testing focuses on verifying that user personnel in the intended operational environment are able to operate, maintain, support, and control the system.

Activity 15: Conduct In-Service Review for Human Factors			
Responsible Agent	Product	Approval Authority	Tools and Aids
Human Factors Coordinator	Assessment of the acceptability of the human-machine interface Post-Deployment Human Factors Assessment Plan	System Engineer	Guidance on conducting human factors assessments In-Service Management Review (ISR) Checklist

Description

Operational suitability and effectiveness are major evaluation factors that are considered in making the decision to place a new capability into operational service. Satisfactory human performance is an integral element of operational suitability and effectiveness. The broad range of human factors engineering issues is addressed during this activity. Also, a plan is formulated to assess and monitor the human-system performance of the new capability following its deployment to the operational environment.

4.8.3.6 Human Factors Engineering Process Outputs/Products

Efforts to manage the human factors engineering program, establish requirements, conduct system integration, and test and evaluate human factors engineering compliance may result in many major and minor human factors engineering outputs and products. These products include human factors input to the primary acquisition documentation (e.g., requirements documents, investment analyses, acquisition program baselines, integrated program plans, specifications, and statements of work) as well as human factors research, studies, and analyses that support program and design decisions and documentation (e.g., human factors risk analyses, human factors benefits analyses, criteria for performance evaluation, prototype designs, and critical task analyses). The human factors engineering activities and their resultant products are described in more detail in the FAA Human Factors Job Aid (and other human factors engineering manuals), but are reflected in five key components of program planning and implementation.

4.8.3.6.1 Human Factors Engineering Planning

Human factors engineering planning involves developing concepts, tasks, completion dates, levels of effort, methods to be used, strategy for development and verification, and an approach to implementing and integrating with other program planning.

4.8.3.6.2 Human Factors Engineering Analysis

Human factors engineering analysis involves identifying the best allocation of function to personnel, equipment, software, or combinations to meet the acquisition objectives. It includes the dissecting functions to specific tasks, analyzing tasks to determine human performance parameters, quantifying task parameters to permit evaluation of human-system interfaces in relation to total system operation, and the identifying high-risk human factors engineering areas.

4.8.3.6.3 Human Factors Engineering Design and Development

Human factors engineering design and development involves converting mission, system, and task analyses data into (a) detail designs and (b) development plans to create human-system interfaces that operate within human performance capabilities, meets system functional requirements, and accomplishes mission objectives.

4.8.3.6.4 Human Factors Engineering Test and Evaluation

Human factors engineering test and evaluation involves verifying that systems, equipment, software, and facilities may be operated and maintained within intended user performance capabilities and is compatible with overall system requirements and resource constraints.

4.8.3.6.5 Human Factors Engineering Management and Coordination

Human factors engineering management and coordination involves coordinating with RMA engineering; system safety; risk management; facilities systems engineering; integrated logistic support; and other human factors engineering functions, including biomedical, personnel, and training.

4.8.3.7 References:

1. FAA Order 9550.8, Human Factors Policy (October 1993).
2. FAA Human Factors Design Standard (May 2003).
3. FAA Human Factors Job Aid (March 1999).
4. MIL-HDBK-759C, Human Engineering Design Guidelines (July 1995).
5. MIL-HDBK-1908, Definitions of Human Factors Terms (August 1999).
6. MIL-HDBK-46855A, Human Engineering Program Process and Procedures (May 1999).
7. Boff, K., & Lincoln J. (Eds.). (1988). Engineering Data Compendium: Human Perception and Performance (Vols. 1- 3). Wright-Patterson Air Force Base, OH: Harry G. Armstrong Aerospace Medical Research Laboratory.
8. Booher, H. R. (Ed.). (1990). MANPRINT: An Approach to Systems Integration. New York: Van Nostrand Reinhold.
9. Booher, H. R. (Ed.). (2003). Handbook of Human Systems Integration. New York: Wiley.
10. Cardosi, K. M., & Murphy, E. D. (Eds.). (April 1995). Human Factors in the Design and Evaluation of ATC Systems Washington, DC: USDOT/FAA.
11. Federal Aviation Administration. (1995). The National Plan for Civil Aviation Human Factors. Washington, DC: Federal Aviation Administration.
12. Meister, D. (1985). Behavioral Analysis and Measurement Methods. New York: John Wiley.
13. National Research Council (1997). Flight to the Future: Human Factors in Air Traffic Control. Washington, DC: National Academy Press.
14. National Research Council (199T). The Future of Air Traffic Control: Human Operators and Automation. Washington, DC: National Academy Press.
15. Salvendy, G. (Ed.). (1997). Handbook of Human Factors and Ergonomics (2nd ed.). New York: Wiley-Interscience.
16. Sanders, M. S., & McCormick, E. J. (1993). Human Factors in Engineering and Design (7th ed.). New York: McGraw-Hill.

17. Wickens, C. D. (1992). Engineering Psychology and Human Performance (2nd ed.). New York: Harper Collins.

18. Wiener, E. L., & Nagel, D. C. (Eds.) (1988). Human Factors in Aviation. New York: Academic Press.

4.8.4 Electromagnetic Environmental Effects

E^3 Engineering is the technical discipline dealing with the safe and efficient operation of electronic devices regarding radiated and conducted electromagnetic emissions. This includes both a given system's ability to deal with such emissions from its operational environment and how the device itself affects that environment.

E^3 activities seek to minimize the limitations of a system due to electromagnetic factors, as well as document limitations and vulnerabilities that remain after a system's deployment.

4.8.4.1 What Is Electromagnetic Environmental Effects Engineering?

E^3 Engineering is a set of Specialty Engineering analyses that relate to electronic systems. Such systems range from electric household appliances to integrated circuits.

The Federal Communications Commission (FCC), responsible for government regulations related to E^3, gives special attention to what it refers to as "digital devices." The FCC defines a digital device as:

> *Any unintentional radiator (device or system) that generates and uses timing pulses at a rate in excess of 9000 pulses (cycles) per second and uses digital techniques . . . .*

In other words, electronic devices using high-speed switching waveforms are digital devices. These devices usually generate significant EMI and shall be designed to conform to government regulations on electromagnetic emissions.

However, E^3 considerations go far beyond government regulations. Manufacturers and developers employ E^3 analyses to ensure proper function of all electronic systems within an operational environment and the compatibility of these with nonelectronic elements of that environment. The analyses also identify potential problems that could arise from changes in the environment.

There are many types of E^3 that may affect the electromagnetic compatibility of a system. Each type is a specialty area unto itself. From a broad perspective, the operational requirement is to properly address the EM environment over the system lifecycle. The following sections discuss the individual elements of E^3. (Note: E^3-related definitions appear in American National Standards Institute (ANSI) C63.14.)

4.8.4.1.1 The Electromagnetic Environment

The Electromagnetic Environment (EME) consists of the systems and other elements (such as humans and nature) that exist within the area where a given system is (or may be) operated. Identifying and describing the EME is a major part of E^3. This involves describing EMI present within the environment and vulnerabilities to systems and other elements of the environment.

In some instances, developers may wish to define the *survivable* EME for a system; that is, the most extreme conditions (EMI present) within which the system may operate safely and without degradation of its function. But whenever possible, it is important to

provide a complete description of the normal EME within which the system, subsystem, or equipment may be required to perform.

4.8.4.1.2 Electromagnetic Compatibility

A key area of E^3 is Electromagnetic Compatibility (EMC). This is the ability of a system to function within its EME and itself and not be a source of troublesome EMI. EMC analyses involve evaluating the EME, all EMI present within that environment, and the new system's own EMI emissions. This data is then used to determine if either the new system or the elements of the operational environment are adversely affected by each other.

FAA-G-2100G, paragraph 3.3.2 Electromagnetic Compatibility, may be invoked as a requirement for acquisitions. It references all appropriate FCC rules and FAA-referenced Military Standards.

EMC considerations are critically important and may be seen as design objectives beyond those required for the basic functional performance of an electronic system. This means that while a system may function properly in the laboratory, problems may occur when it is deployed within a different EME.

There are two general types of emissions to consider in evaluating EMI: conducted emissions and radiated emissions. Conducted emissions are electric currents transferred through physical coupling, such as noise fed back into a device's alternating current (Alternating Current (AC) power system. Radiated emissions are electromagnetic (EM) waves emitted intentionally or unintentionally that may be unintentionally received by other systems. Wires transmit and receive EM signals like intentional antennas. Switching waveforms in circuits generate a wide band of EM emissions.

4.8.4.1.3 Electromagnetic Susceptibility

EM Susceptibility (EMS) specifically deals with a system’s weaknesses or lack of resiliency to certain EM conditions.

A system may likely be exposed to different operational EMEs during its lifetime. A system that suffers degradation within certain potential EMEs is said to be *vulnerable*. A vulnerability analysis is usually required to determine the operational impacts of laboratory-observed susceptibilities.

A *susceptibility* is a particular condition that causes a system to be degraded. For example, conducted susceptibility refers to a system's inability to withstand an infusion of noise into its power lines. Devices that run on standard AC power shall not be susceptible to sudden brief spikes or losses of power if that the power system is affected by lightning or other surges.

4.8.4.1.4 Hazards of Electromagnetic Radiation

Hazards of EM Radiation (RADHAZ) are areas of E^3 that deal with specific types of dangers related to radiated EM waves. Hazard of EM Radiation to Fuels (HERF) is a RADHAZ area dealing with fuels that may be present within an EME. An EM field of sufficient intensity may create sparks that may ignite volatile combustibles, such as fuel. (i.e., EM radiation may induce a current in a conductive material, and sparks are formed in the air gap between two conductors.) It is difficult to locate all potential antennas and spark gaps within an EME, so it is necessary to keep the power densities of EM fields within safety margins when fuels are present.

Hazard of EM to Personnel (HERP) is another important area of RADHAZ; it deals with the dangers of radiation to humans within the EME. Microwave absorption by a human causes heating of the body. At high power levels, such as from radar towers, this may be hazardous. And EM waves in the x-ray range and higher (in terms of frequency) may cause ionization, even at low power levels. RADHAZ precautions help ensure safety for the nonelectronic elements of an EME.

4.8.4.1.5 Electromagnetic Pulse

An EM Pulse (EMP) is an intense burst of EMI caused by a nuclear explosion. This pulse may damage sensitive electronic systems or cause them to temporarily malfunction.

4.8.4.1.6 Electrostatic Discharge

An Electrostatic Discharge (ESD) is an unintentional transfer of static electricity from one object to another. Static voltage transferred from a human to a device (e.g., voltage generated by walking across a carpet) may be as high as 25 kilovolts. The brief currents created may damage or cause malfunction of integrated circuits and other electronics.

4.8.4.1.7 Lightning

The phenomenon of lightning gets special attention within E^3 because of its tremendous power levels and multiple effects. Lightning effects are categorized as *direct* (physical effects) and *indirect* (induced electrical transients and interaction of the EM fields associated with lightning).

4.8.4.1.8 Precipitation Static

Precipitation Static (P-Static) is the buildup of static electricity resulting from an object's exposure to moving air, fluid, or tiny solid particles (e.g., snow or ice). It may cause significant ESD and is a particularly important consideration regarding systems aboard aircraft and spacecraft.

4.8.4.2 Why Perform E^3 Activities?

The following sections discuss the key reasons for incorporating E^3 activities into the SE process.

4.8.4.2.1 Government Regulations

The FCC develops and enforces government regulations relating to E^3. Before a new electronic device is to be sold in the United States, it shall meet the FCC's standards. These standards are detailed in Rules and Regulations, contained in Title 47 (Part 15) of the Code of Federal Regulations.

FCC requirements focus on a system's generated EMI, rather than its EMS. Limits are imposed on the conducted and radiated emissions of digital devices. Radiated emissions are regulated strictly in terms of the electric field. Most NAS-related electronic/RF devices fall under FCC Class A (commercial, industrial, or business). Regulations are less stringent for Class A than for Class B (household) devices.

Government regulations change frequently, so it is important to obtain the most current requirements. Information is available from the FCC Web site www.fcc.gov. The FCC may request a sample device of a new system to test.

4.8.4.2.2 System Performance and Cost of Redesign

While manufacturers and developers strive to meet government regulations, , they may impose additional E^3 requirements on a new system to enhance product performance and customer satisfaction. Government E^3 requirements by no means guarantee a new system's compatibility with its intended operational environment. Thus, it is up to manufacturers and developers to consider the EME for a new system, the impacts of the system's own EMI on that environment, and the system's EMS in order to avoid potential problems that FCC regulations are unable to predict or prevent.

Developers and manufacturers who consider potential E^3 problems from the start may avoid costly redesign later. The earlier in a system's lifecycle that a problem is identified, the less the cost of correcting it is likely to be. For instance, if a problem with EMC is discovered after a new system has been deployed, the system may have to undergo extensive redevelopment. However, if this problem had been determined during the design and planning stage, it could have been addressed in the requirements before manufacture had begun, saving both significant time and resources.

4.8.4.2.3 Hazard Prevention

Hazards of EM radiation on fuels and personnel (HERF, HERP) are important considerations. These issues may be included as part of Safety Risk Management activities.

4.8.4.2.4 International Considerations

EMI is increasing throughout the world. Systems that may be used outside of the United States, such as avionics, shall be able to deal with types and intensities of EMI present in other countries that may be different from conditions in the United States. It is recommended that such systems be designed with special attention given to minimizing vulnerability to EM radiation.

Also, it is recommended that consideration be given to the possibility of intentional jamming, which creates significant EMI.

4.8.4.2.5 Sources of Information on Electromagnetic Environmental Effects

- FCC www.fcc.gov
- ANSI/IEEE standards.ieee.org
- OMB Circular A-11
- Joint Spectrum Center www.jsc.mil/jsce3/e3prg.asp (military)
- FAA fast.faa.gov

4.8.4.3 Analyses of Electromagnetic Environmental Effects

While Section 4.8.0.3 describes the Specialty Engineering process in general terms, this section specifically discusses the various E^3- related analyses. Not all E^3 analyses discussed, however, are important for a given system. It is recommended that it be determined during planning, which analyses are worth the time and resources and which are not.

It is recommended that E^3 analyses be performed on COTS systems as well as new systems to ensure compatibility with the EME within which these systems or subsystems may be used. The amount of detail involved with E^3 analyses increases with each subsequent phase of the SE lifecycle. Measurement procedures for evaluating a product's emissions during low-level technical analyses shall be clearly spelled out. It shall be understood how the results are to be interpreted. The EME may undergo appreciable changes at any point during a system's lifecycle. Thus, E^3 analyses shall be reconducted to ensure continued EMC of *each* system within the EME.

4.8.4.3.1 Description of the Operational Electromagnetic Environment

Before any EMC analyses are conducted, it is necessary to describe the EME within which the system in question may perform. This means detailing all sources of EMI in the operational environment. EME contributors are gauged by the power levels and frequencies of their emissions and their locations (with respect to the new system).

In some cases, it may also be advisable to denote inherent susceptibilities associated with other systems within the EME.

An existing OSED document may be useful as a starting point for an EME description. The OSED contains information about the operational environment and the systems/subsystems associated with the system under analysis. However, the OSED may not describe all EME contributors.

Optionally, a description may be drawn up of the maximum survivable EME conditions in which the system shall be able to function without degradation. This is useful in cases in which a specific operational EME may not be identified (e.g., the system may have numerous and appreciably different operational EMEs to which it is expected to be exposed).

4.8.4.3.2 Electromagnetic Compatibility Analyses

EMC analyses identify compatibility issues relating to radiated and/or conducted emissions. This involves evaluating how the EME and the system affect each other in terms of EMI.

It is useful to calculate the system's *electrical dimensions* before an EMC analysis is conducted. This is done to determine whether or not simple mathematical methods (e.g., Kirkchoff's Laws) are sufficiently accurate for an EMC analysis. If the system is *electrically large*, then simple mathematics are insufficient, and Maxwell's Equations shall be employed. These are a set of differential equations that describe an electric field as three-dimensional parameters (x, y, z) and time (t).

4.8.4.3.2.1 Federal Communications Commission Regulations

It is convenient to address FCC compliance issues for EM emissions during EMC analyses, since both deal with the system's EMI. While actual testing to verify that FCC requirements are met may not occur until a system is built, incorporating these regulations into requirements from the beginning of system development helps to mitigate compliance problems later.

4.8.4.3.3 Analyses of Hazards of Electromagnetic Radiation

RADHAZ analyses are conducted only when they have relevance for a particular system and its environment. For example, if there are no fuels present within the operational EME, an HERF analysis is unnecessary. It is recommended that the types of RADHAZ analyses (if any) to be performed be determined from the EME description.

4.8.4.3.4 Electromagnetic Susceptibility Analyses

As with RADHAZ, specific susceptibility analyses are conducted only when they have relevance. Each analysis requires time and resources, so it is impractical to invest in an analysis that has no significance for the system and its EME. Susceptibility analyses include:

- Conducted Susceptibility (AC power lines)
- ESD Susceptibility
- Susceptibility to Lightning
- P-Static Susceptibility
- EMP Survivability

4.8.4.4 Outputs and Products of Electromagnetic Environmental Effects

It is important to employ E^3 analyses and predictions during all phases of an electronic system's lifecycle. Figure 4.8-1 illustrates the fundamental Specialty Engineering process and its outputs. The following sections link the outputs of E^3 activities to the overall System Engineering process. However, it is important to note that all E^3 analyses, like other Specialty Engineering analyses, shall be documented in a DAR.

4.8.4.4.1 Requirements

Most E^3 activities result in requirements that feed the Requirements Management process. This includes the Mission Need Statement, Statement of Work, specifications, and all performance-based requirements.

4.8.4.4.2 Concerns and Issues

It is recommended that E^3 activities—in addition to identifying necessary requirements—also identify potential problems that may surface later in a system's lifecycle. It is also good practice to document identified system susceptibilities that are not significant enough to require correction. These issues are included with concerns and issues, which feed the Risk Management process (Section 4.10).

4.8.4.4.3 Verification Criteria

It is critical to provide verification criteria to ensure that stated E^3 performance requirements are met. It is also important to provide detailed information describing how E^3 testing is performed and how test results are to be interpreted. This feeds the Validation and Verification process (Section 4.12).

4.8.4.4.4 Solutions to Problems of Electromagnetic Environmental Effects

EMC and EMS problems may be corrected through a number of means, including shielding, emission suppression components, and/or modification of the operational environment. However, some problems may not be directly correctable, potentially forcing extensive and costly redesign of the product. This is why it is beneficial to consider E^3 issues early in a system's development.

[Section 4.8 Version 2.0 09/30/03]

4.8.5 Quality Engineering — Reserved

4.8.6 Information Security Engineering

Information Security Engineering (ISE) is a Specialty Engineering discipline within Systems Engineering. It is recommended that Systems/security engineers and program managers use the following reference documents for further information regarding planning and conducting ISE:

- FAA Policy Order 1370.82 describes roles and responsibilities related to certification and accreditation (C&A) of IT products and systems within the FAA
- FAA Information Systems Security (ISS) Handbook outlines how security engineering activities, including producing C&A products, shall be conducted, including specific work products
- FAA AMS provides acquisition policy and guidance about when, how, and in what sequence security engineering activities and work products are to be done during the system lifecycle

The FAA directives and guidance incorporate necessary federal and industry policy and standards. The following ISE section describes why security engineering is important, and it describes what steps and processes shall be followed within the FAA to integrate system security into the overall system engineering process for an FAA system.

4.8.6.1 Perform Information Security Engineering

Federal legislation, such as the Clinger-Cohen Act of 1996, and the Federal Information Security Management Act (FISMA) of 2002, establish a clear legal basis for establishing information security risk management practices for federal IT resources. To implement the legislative mandate within the Executive Branch, the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, establishes policy for managing federal information resources.

OMB includes procedural and analytic guidelines for implementing specific aspects of these policies as appendices. The Circular A-130 Appendix III, Security of Federal Automated Information Resources, establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and requires that an agency official authorize use of the information technology system.

The FAA Order 1370.82 and the ISS Handbook have implemented the Security Certification and Authorization Package (SCAP), which documents the security requirements and the validation and verification of those requirements as the basis for security authorization by the proper FAA official. The SCAP implements key aspects of FISMA and OMB A-130.

Chapter 10 of DOT Order 1350.2, Departmental Information Resources Management Manual, implements OMB guidance for DOT, while the FAA implements departmental direction in FAA Order 1370.82 and applicable portions of the AMS.

Several factors drive the FAA focus to develop and implement rigorous ISS (see Figure 4.8-12):

- The AMS and FAA practice call for using or adapting commercially available IT products to satisfy mission needs of the agency. Referred to as COTS, these products may contain vulnerabilities that, unless properly engineered and managed, may produce significant risks to the services, capabilities, and functions a system is expected to perform in meeting FAA mission needs.

- The pervasiveness of networked information and the increased interconnectivity of FAA systems significantly broaden the FAA's exposure to malicious activities from a variety of sources. Expanded services and capabilities brought about by networking and automation enable improved performance and efficiency; yet may dramatically expand vulnerabilities to systems' confidentiality, integrity, and availability unless security is properly addressed.

- Global terrorism and our post 9/11 world drive the need for more active, capable and responsive defense of the United States. The FAA is modernizing its capabilities to ensure that the aviation transportation system is adequately protected from risks to the safety and security of the flying public. Proper ISE ensures that information exchange has appropriate security controls, features, and services. Security controls support continuity of operations for IT systems under a range of conditions that increasingly involve homeland security defense and disaster response as inherent to FAA services and capabilities.

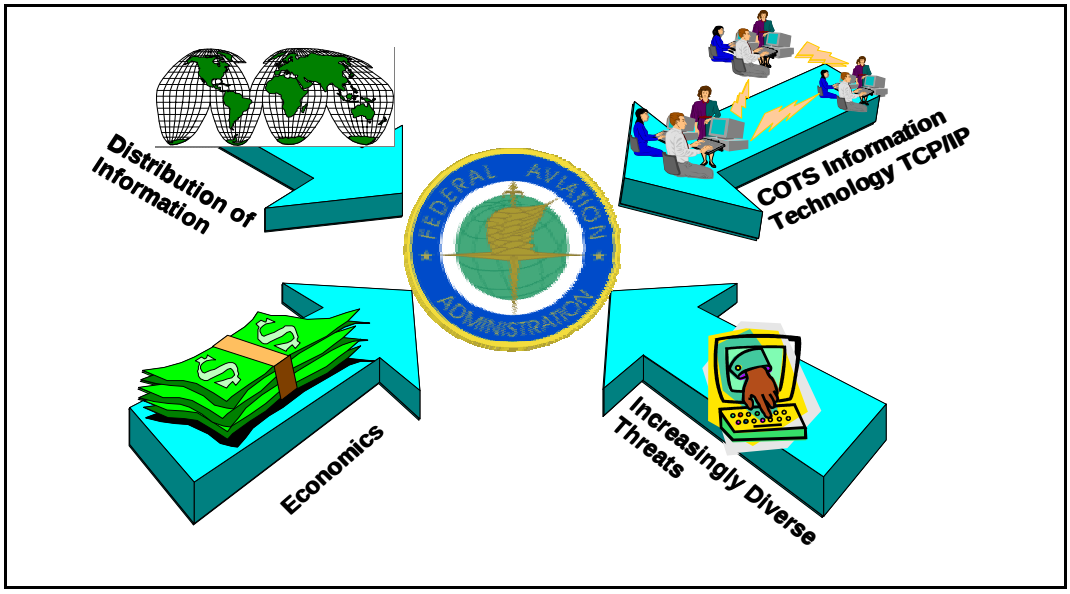


Figure 4.8-12. Force of Change Driving Security

The above factors drive the FAA toward more thorough and disciplined implementation of ISE throughout the system lifecycle.

Including security early in development and acquisition of FAA systems usually results in lower costs and more effective security features when compared to adding security features after the systems have entered service. The SEM presents a security-engineering framework that supports all phases of the AMS, from early planning to contract closeout and/or system disposal. The next section outlines the general principles for ISE.

4.8.6.2 Information Security Engineering Principles

Similar to systems safety engineering, the concept of risk management is central to conducting effective and complete ISE. Security risk management includes assessment, mitigation, monitoring, and control of security risks throughout the life of every FAA information technology system. From the ISE perspective, combining the likelihood of a particular threat exploiting or triggering a particular system vulnerability produces a security risk (FAA ISS Handbook). Proper ISE seeks an acceptable level of security risk, also referred to as "risk," at an acceptable cost. An acceptable risk is one determined to represent an acceptable condition of potential

loss, damage, or disruption for the FAA mission. Adequate security controls are like insurance—the system sponsor or developer spends enough resources to mitigate the risk of loss, damage, or disruption to an acceptable level. However, to be cost-effective, it is recommended that the sponsor or developer not spend more than the risk of loss, damage, or disruption.

In conducting ISE for a system, consider the following important points (see also Figure 4.8-13):

- Security shall always consider the operational environment of the system and the system's contribution to the FAA mission and services. Security shall include consideration of continuity of operations and disaster response by the system in its operational environment.
- ISE shall consider the personnel and physical security features and services, including management and administrative controls, procedures, and processes.
- It is recommended that ISE use existing SE and AMS products and processes as a cost-effective means of building and improving ISE practices.
- Security engineers shall collaborate with the Integrated Requirements Team (IRT) and system stakeholders. Collaboration with the IRT, including system safety engineers, may avoid unnecessary and duplicative security requirement statements and costly, specialized controls for security services that may be effectively handled by other system features, such as procedures, physical controls, or interfacing systems/services.

Chapter 3 of the FAA ISS Handbook describes how to determine ISS risks using the Security Risk Management Process in Figure 4.8-14. The figure illustrates a closed-loop process for managing risk at any phase or point in the system lifecycle. It is recommended that this process be applied very early in the system development so that security requirements are defined upfront. There is further information in this section about applying this process during phases of the AMS to produce ISE products. Also, the ISE supports the overall Risk Management process of (Section 4.10).

It is recommended that each system developer and system owner apply the ISE risk-management process as a primary tool for performing and contributing to other SE activities, analyses, plans, and products. Figure 4.8-15 illustrates how ISE supports, and is supported by, other SE practices.

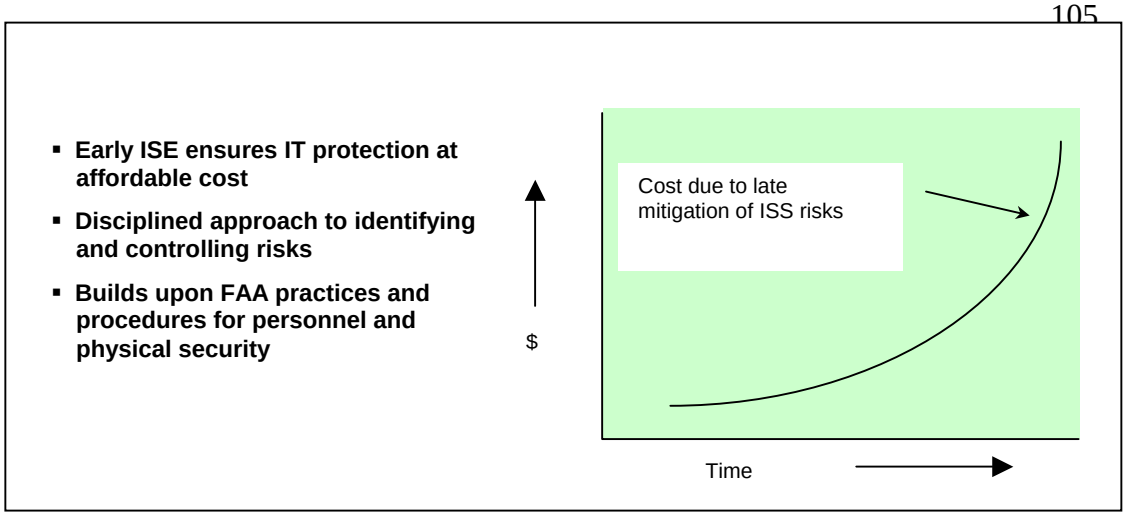


Figure 4.8-13. Benefits of Information Security Engineering

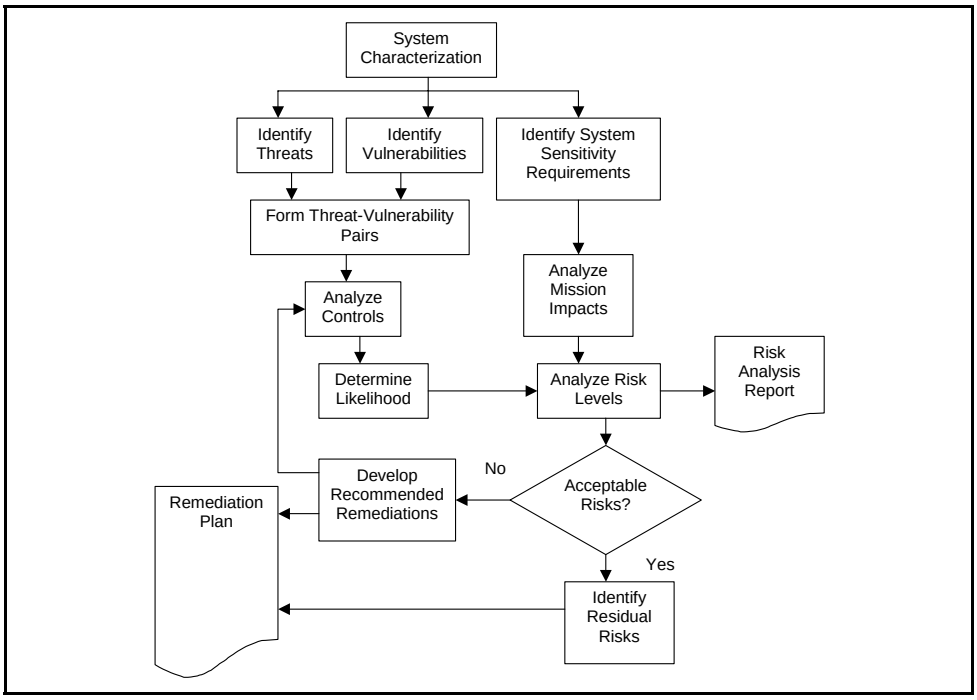


Figure 4.8-14. System Security Risk Management Process

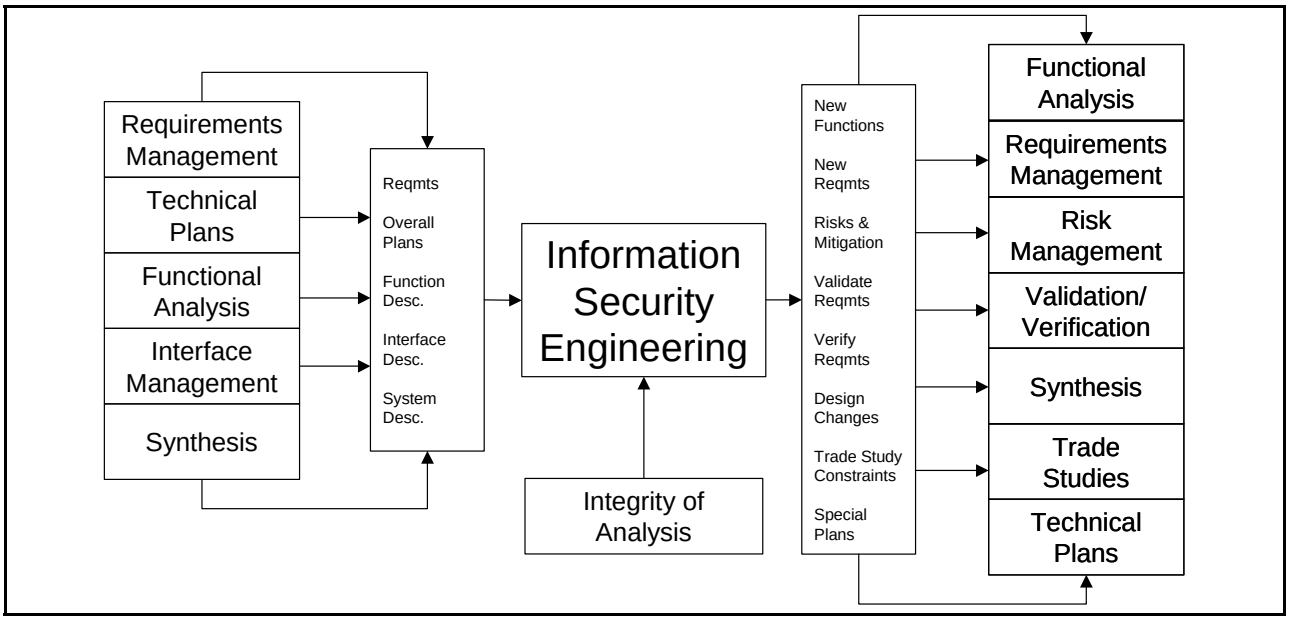
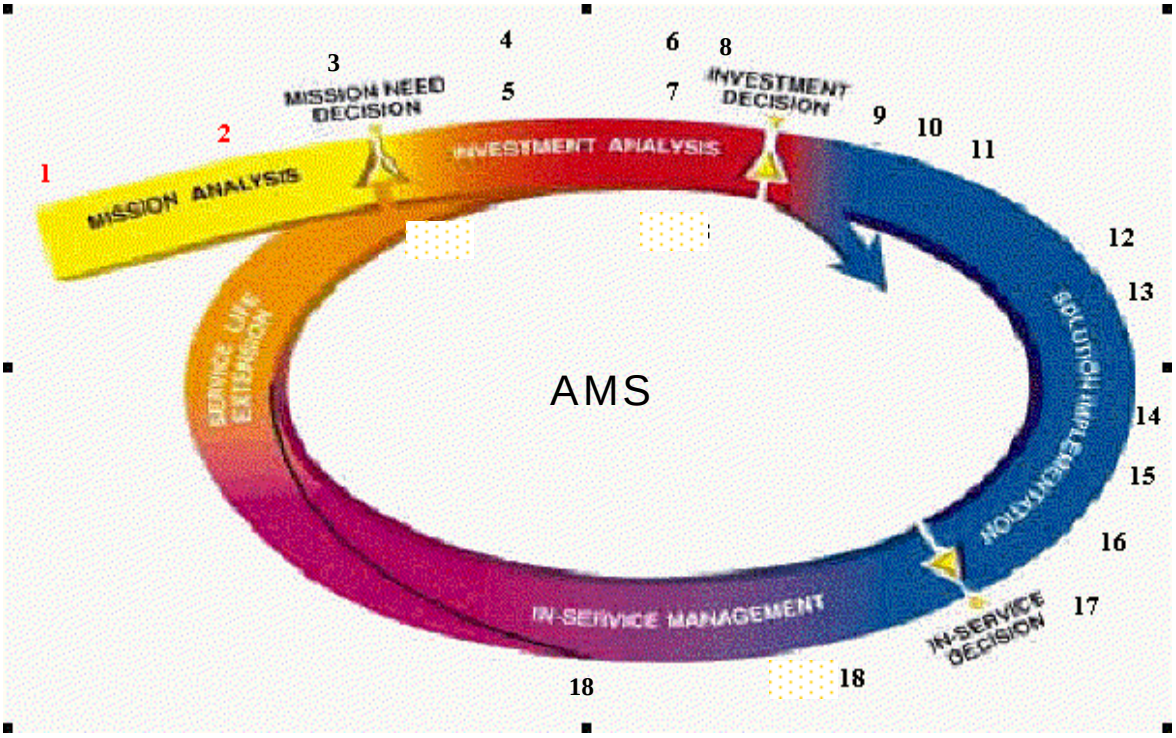


Figure 4.8-15. ISE Relationship to Other System Engineering Processes

Early application of ISE principles may reduce lifecycle costs and improve overall SE. ISE uses existing capabilities of many COTS products, but relies on early application of ISE processes, tools, and security risk management practices. Also, ISE leads to identifying high-risk security elements earlier in the system lifecycle. When high-risk elements are found and mitigated early, it is simpler and less expensive to make corrections. The outputs of the ISE process feed other SE processes, improving the overall SE of the system.

4.8.6.3 Information Security Engineering Process Tasks

The AMS Lifecycle integrates a continuum of ISE processes and products. Figure 4.8-16 shows what security analyses and products are performed relative to the AMS phases and decision milestones. The representation is notional. Each program or Product Team may need to tailor its activities to meet its program milestones. The security analyses and activities are sequenced to support the phased decisions of the AMS. It is recommended that each program or Product Team use its respective SEMP and security planning to tailor its security risk management program. National Institute of Standards (NIST) Special Publication (SP) 800-18, Guide for Developing Security Plans for Information Technology Systems, provides the basis for security planning referenced in the FAA ISS Handbook.



Legend
ISE Risk Management Process aligned with AMS

1. Basic Security Policy
2. MNS Threat Stipulation and Begin Detailed Security Engineering Activities
3. CONOPS and Preliminary Security Requirements or Protection Profile
4. Preliminary Vulnerability Assessment
5. Preliminary Risk Assessment
6. Updated Vulnerability Assessment
7. Updated Risk Assessment and Risk Mitigation
8. Updated CONOPS and Security Requirements or Protection Profile
9. Security Requirements Integrated with System Requirements
10. Integrated Security Architecture and Design
11. Final ISSP
12. Security Test Planning and Procedures
13. User's Guide, Training and Contingency Plans
14. Integrated Security Testing with SAT

15. Integrated Security with OT&E
16. Final Security C&A Documents
17. Security Authorization/Accreditation
18. Tech Refresh and Upgrade Planning

Numbered items correspond to AMS Lifecycle diagram numbers, above

Figure 4.8-16. Security Risk Management Relative to the AMS

The following paragraphs outline in greater detail. The AMS and the ISS Handbook contain further guidance.

- **Mission Analysis Phase**

  Conduct Preliminary Risk Assessment and generate high-level System/Mission Requirements, resulting in a succinct, qualitative description of the basic security needs of the system and a set of high-level ISS requirements that are derived from the Mission Needs Statement, concept of operations, and the OSED. Assess criticality of data and systems to FAA mission and service.

- **Investment Analysis Phase**

  – Confidentiality, Integrity, and Availability Requirements Analysis — identify the protection requirements through an analysis of laws and regulations that define baseline security and consider functional and other security requirements. Apply and refine the criticality assessment from Mission Analysis phase.

  – Security Risk Assessment Update — update the preliminary risk assessment based on the results of the confidentiality, integrity, and availability requirements. Use Trade Studies (Section 4.6) to assess cost-effective security controls that may form the basis for desirable system security requirements. Tradeoff analyses may be warranted to assess alternative control measures, including procedural, physical, and personnel measures.

  – Analysis of the Level of Assurance Required — address how much confidence is needed and that the NAS security is to work in an integrated fashion, correctly and effectively. Assurance may be gained through many techniques, including, among others, conformance testing and validation suites, or evaluations by another vendor.

  – Coordinate Stakeholder, Certifier, and Authorization Review — for this phase of development, ensure a technically qualified person certifies that the security controls on the system, application, or networks meet the NAS ISS requirements.

  – Specification and SOW — based upon the Investment Analysis Phase, provide ISS constraints and requirements to Requirements Management (Section 4.3) as input for final requirements, specifications, and SOW development.

  – Evaluation Proposals — support Trade Studies (Section 4.6), Synthesis (Section 4.5) and Validation (Section 4.12.1) in assessing the minimum ISS requirements for solicitation information requests SIR and evaluating alternative solutions that are proposed.

  – Performance Measurement and Monitoring — Using results from ISS requirements, trade studies, synthesis, and Integrated Technical Planning (Section 4.2), identify effective measures for ISS performance, status, and assurance. Measures may be useful for the applicable phase of acquisition and system development.

- **Solution Implementation Phase**
  - Security Risk Assessment Update — update the assessment based upon the expected ISS functional and assurance controls from the chosen solution. Support Validation (Section 4.12.1) and Synthesis (Section 4.5) to assess controls and assurance as being cost effective and meeting the ISS requirements. Use Requirements Management (Section 4.3) to mitigate security risk to acceptable levels.
  - Information Security Certification and Authorization — use the results of ISE activities, including related system engineering elements like Integrated Technical Planning (Section 4.2) that includes CONOPS, Synthesis (Section 4.5), Validation and Verification (Section 4.12), and Lifecycle Engineering (Section 4.13) to collect and document ISE for C&A. The ISS Handbook provides templates for collecting and presenting C&A documentation.
- **In-Service Decision and In-Service Management Phase**
  - Stakeholder, Certifier and Authorization Review — ensure a technically qualified person certifies and authorizes that the security controls on the system, application, or networks meet the NAS ISS requirements.
  - Performance Measurement and Monitoring — update ISS measures, metrics, and monitoring. Ensure that monitoring ISS performance and assurance for the respective NAS System has not degraded. Assess changes in the environment and system for previously unforeseen risks from new threats and vulnerabilities. Plan and take corrective action as necessary.
- **Service-Life Extension and/or Closeout**
  - Update the Security Plan — ensure security plans evolve with the system. Conduct periodic C&A, consistent with guidance of FAA ISS Order 1370.82.
  - Update ISS requirements — update risk assessment based upon performance measurement and monitoring of In-Service Management. Identify updated and/or new ISS requirements for Service-Life Extension.
  - Archive Information — retain information as necessary keeping in mind legal requirements and future technology changes that render the retrieval method obsolete.
  - Sanitize Media — ensure data is deleted, erased, and written over as necessary.
  - Dispose of Hardware and Software — dispose of the hardware and software as directed by ISS Policy.

The ISE processes and products may also be represented as a series of steps. To satisfy the objectives of each step, consistent with Section 4.8.0.3, it is recommended that the General Specialty Engineering Process Tasks be used. Figure 4.8-17 indicates the ISE steps and shows the relationship of the General Specialty Engineering Tasks to the ISE process. Each program, IPT, or Product Team developing or acquiring IT systems shall institute a Security Risk Management Process that includes risk assessment, risk mitigation, evaluation and assessment, as recommended by NIST SP 800-30, Risk Management Guide for IT Systems. The ISE process steps (Figure 4.8-17) are mapped to the AMS lifecycle by Table 4.8-13. The legend in Figure 4.8-17 indicates the Specialty Engineering Tasks that apply to each ISE process step/activity, as the risk management process is applied throughout the lifecycle.

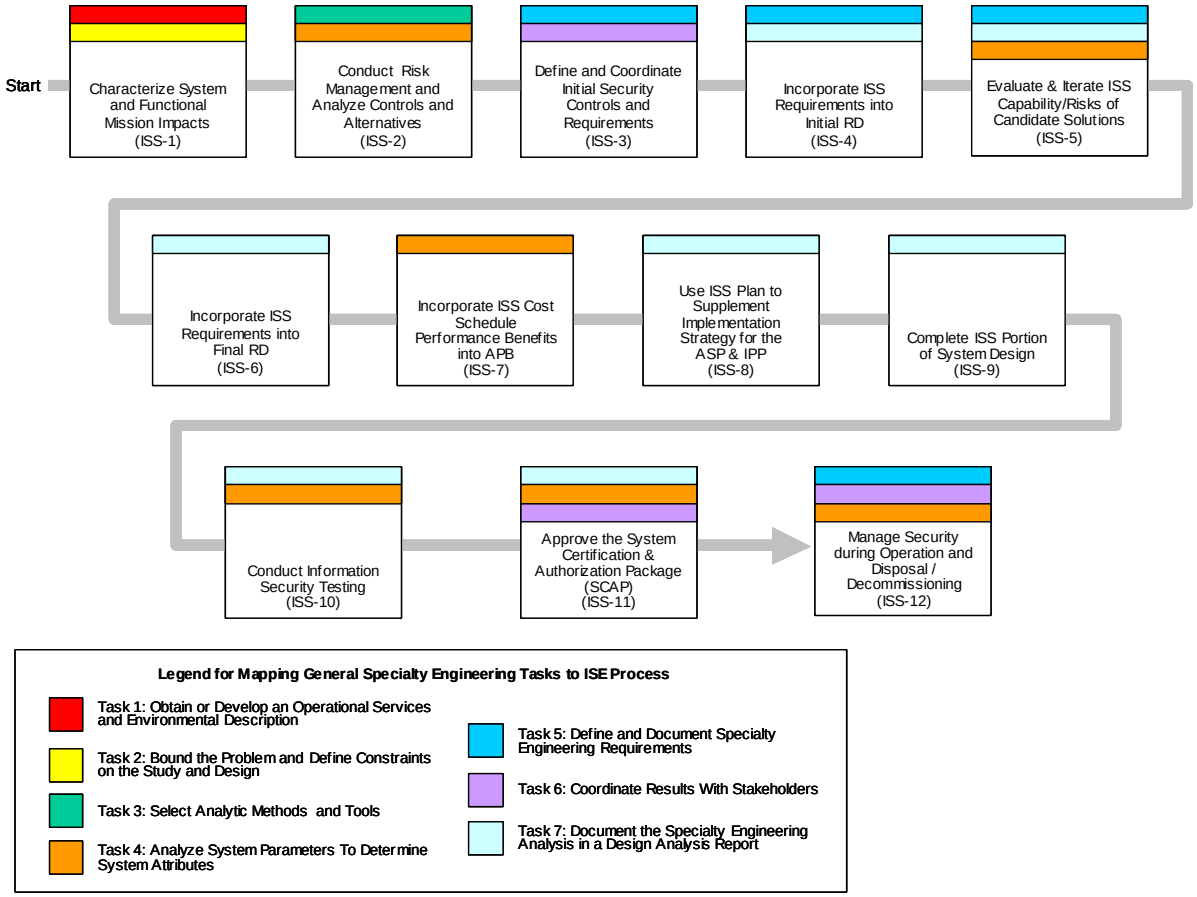


Figure 4.8-17. ISE Process with General Specialty Engineering Tasks Applied

Figure 4.8-14, System Security Risk Management Process, contains all the steps of NIST SP 800-30. Risk management is an iterative process that shall be embedded into each major phase of systems development, and involves the steps outlined in Figure 4.8-14.

- System Characterization
- Threat Assessment
- Vulnerability Assessment
- Analysis of Controls
- Likelihood Determination
- Assessment of Mission Impact
- Analyze Risk Levels
- Risk Mitigation, or Recommended Controls
- Identification and Documentation of Residual Risk

Additionally, the program, IPT, or Product Team Security Risk Management Process shall provide outputs and products as described within the ISS Handbook and summarized in the following section. Each program, IPT, or Product Team shall plan and provide for support of the products defined in Table 4.8.6-3, as a part of system lifecycle acquisition and support.

4.8.6.4 Information Security Engineering Outputs and Products

The ISE process generates the activities and products described in the next sections.

4.8.6.4.1 Program Planning

It is recommended that the program, Product Team, and system sponsor/owner have a System Security Plan (SSP), which is to evolve during the system's lifecycle. The ISS Handbook provides a template for developing the SSP. It is recommended that the SSP evolve with the system development through update and revision based on risk management activities that address growing understanding of how risk requirements for the system may be satisfied. Early in development, the SSP addresses threats and needs of the system with an operational security assessment that reflects the output of the OESD. The risk management process (Figure 4.8-14) shall be applied through each phase of development. To further guide planning, Table 4.8-13 relates the AMS security risk management activities to the ISE Process. Analysis products outlined in Paragraph 4.8.6.4.2 below are used to update the SSP.

Table 4.8-13. Mapping AMS Security Risk Management Activities to ISE Process

AMS Security Risk Management Activities	ISE PROCESS STEPS
1. Basic Security Policy	ISS-1: Characterize System and Functional Mission Impacts
2. MNS Threat Stipulation and Begin Detailed Security Engineering Activities	ISS-2: Conduct Risk Management and Analyze Controls and Alternatives
3. CONOPS and Preliminary Security Requirements or Protection Profile	ISS-3: Define and Coordinate Initial Security Controls and Requirements
4. Preliminary Vulnerability Assessment	ISS-2: Conduct Risk Management and Analyze Controls and Alternatives
5. Preliminary Risk Assessment	ISS-2: Conduct Risk Management and Analyze Controls and Alternatives
6. Updated Vulnerability Assessment	ISS-2: Conduct Risk Management and Analyze Controls and Alternatives
7. Updated Risk Assessment	ISS-2: Conduct Risk Management and Analyze

AMS Security Risk Management Activities	ISE PROCESS STEPS
	Controls and Alternatives
8. Updated CONOPS and Security Requirements or Protection Profile	ISS-4: Incorporate ISS Requirements into Initial RD ISS-5: Evaluate and Iterate ISS Capability/Risks of Candidate Solutions ISS-6: Incorporate ISS Requirements into Final RD
9. Security Requirements Integrated with System Requirements	ISS-8: Use ISS Plan to Supplement Implementation Strategy for the ASP & IPP
10. Integrated Security Architecture and Design	ISS-8: Use ISS Plan to Supplement Implementation Strategy for the ASP & IPP
11. Final ISSP	ISS-8: Use ISS Plan to Supplement Implementation Strategy for the ASP & IPP ISS-9: Complete ISS Portion of System Design
12. Security Test Planning and Procedures	ISS-10: Conduct Information Security Testing
13. User's Guide, Training and Contingency Plans	ISS-10: Conduct Information Security Testing
14. Integrated Security Testing with SAT	ISS-10: Conduct Information Security Testing
15. Integrated Security with OT&E	ISS-10: Conduct Information Security Testing
16. Final Security C&A Documents	ISS-11: Approve the SCAP
17. Security Authorization/Accreditation	ISS-11: SCAP
18. Tech Refresh and Upgrade Planning	ISS-12: Manage Security during Operation and Disposal / Decommissioning

4.8.6.4.2 Analysis Products

The ISS Handbook highlights how ISE work products are used to validate and verify the security requirements of a given system. The work products are generated according to the individual SSP for each FAA service/domain/system. The ISS Handbook provides templates to guide collection of analysis into products used for security accreditation of the service/domain/system by the responsible FAA approving authority, consistent with FAA ISS Policy Order 1370.82.

Table 4.8-14, ISE Risk Assessment Matrix, provides a means of analyzing individual risks and determining the need for mitigation or risk-reduction measures. The matrix reflects the level of risk associated with the **likelihood** of a given threat-source exercising a given vulnerability and the **impact** of that threat source successfully exercising that vulnerability. Risks to IT systems arise from events, such as the following:

- Unauthorized (malicious or accidental) disclosure, modification, or destruction of information
- Unintentional errors and omissions
- IT disruptions due to natural or man-made disasters
- Failure to exercise due care and diligence in implementing and operating the IT system

To use the matrix, apply the determined **Likelihood** value generated during the System Security Risk Management Process (Figure 4.8-14) for each threat source and apply the system's overall **Impact** rating obtained similarly. Locate the **Likelihood** value in the vertical column and locate the **Impact** rating in the horizontal column. The **Risk Level** is where the two values intersect.

Table 4.8-14. ISE Risk Assessment Matrix

Likelihood	1 Minimal	2 Minor	3 Major	4 Serious	5 Catastrophic
5 Near Certainty	LOW	MEDIUM	HIGH	HIGH	HIGH
4	LOW	MEDIUM	MEDIUM	HIGH	HIGH
3	LOW	MEDIUM	MEDIUM	MEDIUM	HIGH
2	LOW	LOW	LOW	MEDIUM	MEDIUM
1 Extremely	LOW	LOW	LOW	LOW	MEDIUM

Impact

Table 4.8-15 lists the products of ISE and references detailed directions on how to develop these products.

Table 4.8-15. Products of Information Security Engineering

Information Security Process Products	How To Reference	How To Apply to the ISE Process
Risk Assessment Report (Includes Threat and Vulnerability Assessments)	FAA ISS Handbook: Chapter 3, Section 3.3 – Risk Assessment Process FAA ISS Handbook: Appendix A-2 – Risk Assessment Report	ISS-2: Conduct Risk Management and Analyze Controls and Alternatives
Risk Mitigation/Remediation Plan	FAA ISS Handbook: Chapter 3, Section 3.4 – Risk Mitigation/Remediation Plan FAA ISS Handbook: Appendix A-3 – Risk Mitigation/Remediation Plan	ISS-2: Conduct Risk Management and Analyze Controls and Alternatives
Information Systems Security Plan	FAA ISS Handbook: Chapter 4, Section 4.1 – Compile an ISS Plan FAA ISS Handbook: Appendix A-4 & A-5 – ISS Plans for General Systems and Major Applications	ISS-8: Use ISS Plan to Supplement Implementation Strategy for the ASP & IPP
Contingency/Disaster Recovery Plan	FAA ISS Handbook: Chapter 4, Section 4.2 – Develop a Contingency/Disaster Recovery Plan FAA ISS Handbook: Appendix A-6 – Contingency and Disaster Recovery Plan	ISS-10: Conduct Information Security Testing
Security Test Plan and Test Results Report	FAA ISS Handbook: Chapter 5 – Remediation Phase FAA ISS Handbook: Appendix A-7 – Security Test Plan and Test Results Report	ISS-10: Conduct Information Security Testing
Executive Summary	FAA ISS Handbook: Chapter 6, Section 6.1.1 – Develop Executive Summary FAA ISS Handbook: Appendix A-8 – Executive Summary	ISS-11: Approve the SCAP
C&A Certificate	FAA ISS Handbook: Chapter 6, Section 6.1.2 – Certification and Authorization Approval Process FAA ISS Handbook: Appendix A-9 – System Certification and Authorization Certificate	ISS-11: Approve the SCAP

4.8.6.4.3 Security Certification and Authorization Package

As outlined (in Paragraph 4.8.6.1 above), FAA Policy Order 1370.82 requires that information technology systems be accredited through an ISS C&A process. To complete the C&A process, the system developer or system sponsor/operator shall submit a SCAP. The SCAP documents the results of validation and verification of security requirements and includes an assessment for the FAA Designated Approving Authority of the level of residual security risk. The principle documents in the SCAP are the Risk Assessment and Mitigation Report, the ISS Plan, Contingency/Disaster Recovery Plan, System Test Plan & Test Results, and the Executive Summary. However, additional ISS documents may need to be created depending on the nature of the system.

The FAA ISS Handbook offers detailed information about the C&A Process and how to go about submitting a SCAP for review. The SCAP is a necessity and an integral step when doing ISE. This is emphasized in ISS-11 of the ISE Process.

4.8.7 Hazardous Materials Management/Environmental Engineering

Hazardous Material Management/Environmental Engineering (HMM/EE) is the subset of Specialty Engineering concerned with the impacts of both the program on the environment and the environment on the program. Federal, state, and local environmental agencies have established mandates that regulate program impacts on the environment. These mandates include requirements to manage hazardous materials and to safeguard natural resources including ambient air, water, and land-based resources. FAA orders and directives (e.g., FAA Order 1050.10, Prevention, Control, and Abatement of Environmental Pollution at FAA Facilities) relate federal environmental regulations to FAA activities and also provide additional environmental requirements specific to NAS operations. Conversely, environmental impacts on programs vary, depending on site-specific environmental conditions that may affect FAA operational requirements. The following sections describe the purpose and general process of HMM/EE within SE.

4.8.7.1 What Is Hazardous Material Management/Environmental Engineering?

HMM/EE is the mechanism applied within the SE process to ensure a program's ongoing compliance with applicable environmental laws. HMM/EE is also the SE process designed to provide early, predeployment planning and coordination to minimize the negative impacts that site-specific environmental conditions may have on a program's operability. Compliance with various environmental regulations is required throughout a program's lifecycle, requiring early and continuous application of HMM/EE principles.

Key considerations are pollution prevention, safety and health (including system safety), cultural and natural resource conservation, public participation, and energy and water conservation It is recommended that additional issues concerning the applicability of state and local agency requirements to federal agencies be referred to the legal office for an evaluation of supremacy clause and sovereign immunity implications. For example, the National Environmental Policy Act requires preparation of an environmental assessment for all proposed federal actions that are not categorically excluded.

Additionally, the Resource Conservation and Recovery Act delineates standards for managing and disposing of hazardous wastes that result from various processes during program operation, and at the end of the program's lifecycle. Through HMM/EE, the breadth of environmental requirements are continuously monitored, and considered, to ensure that FAA's programs take the steps to maintain compliance.

HMM/EE processes also highlight the impacts that environmental conditions and site-specific characteristics may have on a program. FAA specifications developed for various types of equipment delineate operating conditions that shall be considered during the program's developmental stages. For example, the general FAA specification for electronic equipment, FAA-G-2100, details the design standards that shall be followed to ensure equipment functionality in environmental conditions of both seismic zones and temperature extremes. HMM/EE verifies that similar standards are considered and adhered to in the SE process to ensure the reliability of systems fielded under unique environmental settings.

4.8.7.2 Why Perform Hazardous Material Management/Environmental Engineering?

HMM/EE is performed to:

- Support reliable, safe, and sustained NAS operations
- Ensure that compliance with FAA, federal, state, and local environmental requirements
- Ensure environmental considerations are included in the acquisition management process
- Track the status of environmental issues with new and existing systems
- Minimize cost and schedule risks through early detection of environmental issues

Through various regulations, such as FAA Order 1050.17, Airway Facilities Environmental and Safety Compliance Program, the FAA has mandated and delineated requirements to comply with applicable environmental regulations. The FAST ensures that these regulations are considered in the acquisition process in AMS Section 2.9.8, Environmental, Occupational Safety and Health, and Energy Considerations:

> *FAA acquisitions are subject to federal environmental, occupational safety and health, and energy management statutes, regulations, executive orders, and Presidential memoranda. Key considerations are pollution prevention, safety and health (including system safety), cultural and natural resource conservation, public participation, and energy and water conservation. Additional issues concerning the applicability of state and local agency requirements to federal agencies should be referred to the legal office for an evaluation of supremacy clause and sovereign immunity implications.*

The following illustrate some of the requirements:

- The National Environmental Policy Act "requires preparation of an environmental assessment or an environmental impact statement for all proposed federal actions that are not categorically excluded. Depending on the results, an environmental assessment can lead to an environmental impact statement or a finding of no significant impact. Following the prescribed review periods, the FAA may make a decision on the federal action."
- Various other environmental laws (e.g., the Federal Facilities Compliance Act) "impose environmental requirements, and sanctions for noncompliance, including civil penalties."
- The Occupational Safety and Health Administration (OSHA) "requires a safe and healthful workplace for all employees, and compliance with OSHA standards."

> *OSHA (29 CFR §1910.28) and GSA (Federal Property Management Regulations) require the FAA to establish and maintain an Occupant Emergency Plan for all FAA facilities. In the event an acquisition program impacts egress routes or fire safety of a facility, the plan must be updated by the program office or the Product Team performing the project.*

- The National Energy Conservation Policy Act "requires energy and water conservation measures for federal buildings, facilities or space."

> *Environmental, safety and health, and energy conservation considerations apply from the beginning of the acquisition lifecycle through product disposal. The Acquisition Program Baseline shall incorporate estimates for the full cost of complying and allow sufficient time for doing so. FAST contains procedural guidance for required actions*

When applied early, HMM/EE identifies applicable environmental requirements to include in development and acquisition of new systems, thereby providing significant savings through risk minimization, cost avoidance, and enhancement of system efficiency. Additionally, consideration of environmental impacts on systems while they are in the developmental stages ensures their functionality in various field conditions.

HMM/EE conducted as part of in-service program management analyzes the impact that engineering changes in the field may have on environmental concerns. As obsolete equipment is removed, HMM/EE ensures that replacement equipment complies with applicable environmental regulations. In particular, decommissioning and removal of obsolete equipment require HMM/EE considerations to ensure that final disposition/disposal is conducted in accordance with applicable environmental requirements. HMM/EE also evaluates the impact that regulatory changes may have on fielded systems.

Programs that fail to fully incorporate HMM/EE principles may have significant impacts on NAS operations. Noncompliant programs may:

- Be removed from service through regulatory enforcement actions
- Require costly post-fielding/retrofit modifications
- Incur fines

Additionally, costs associated with new equipment fielding, and obsolete equipment disposition and disposal may lead to significant budgeting issues if they are not considered during the program development phase.

4.8.7.3 Hazardous Material Management/Environmental Engineering Process Tasks

HMM/EE follows the process tasks outlined in General Specialty Engineering Process Tasks (Paragraph 4.8.0.3).

4.8.7.4 Hazardous Material Management/Environmental Engineering Outputs and Products

Throughout the various phases of the system acquisition process, HMM/EE is used in developing and reviewing key documents. Early implementation of HMM/EE principles is essential to minimize the impact that environmental requirements may have on system costs and operations. During the preliminary activities, such as development of mission needs, requirements, and investment analysis, HMM/EE is used to make initial assumptions and estimates on how environmental considerations may come into play throughout the various lifecycle stages.

During the solution implementation phase of the acquisition process, HMM/EE is used to shape portions of the SOW and system specifications documents as they relate to environmental

considerations. For example, SOWs may be developed to support FAA efforts to meet National Environmental Policy Act demands that federal agencies minimize use of toxic substances in its operations.

During the in-service management phase of the system lifecycle, HMM/EE is used to address issues that may arise unexpectedly in the field. In particular, older pieces of equipment that may not have been developed with HMM/EE in mind may require corrective measures to meet environmental regulations. Additionally, the set of ever-changing environmental regulations may impact the way systems are operated. Finally, as old systems are decommissioned, HMM/EE is necessary to ensure that all disposal actions consider applicable environmental laws.

4.8.7.4.1 Program Integration

As part of the SE process, HMM/EE provides expertise for developing various documents required for program integration. Throughout the various lifecycle phases, HMM/EE ensures that all applicable regulations and environmental conditions are properly addressed so that their impacts are accounted for appropriately. For example, HMM/EE would support development of the IRD, keeping in mind environmental regulations that require federal agencies to verify that their activities do not negatively impact certain ecosystems. Similarly, HMM/EE's role in developing IPPs, SOWs, Disposition/Disposal Plans, and other such documents generate comments and input concerning the compliance requirements that may impact the progress of program implementation, and FAA's compliance status and future liabilities.

Included in the HMM/EE aspects of program integration is a functional analysis of the OSED (see Section 4.4 (Functional Analysis)). This portion of the functional analysis ensures that the environmental conditions that the various systems face are fully considered and that plans are appropriately developed to address identified conditions.

Figure 4.8-18. depicts HMM/EE Inputs and Outputs.

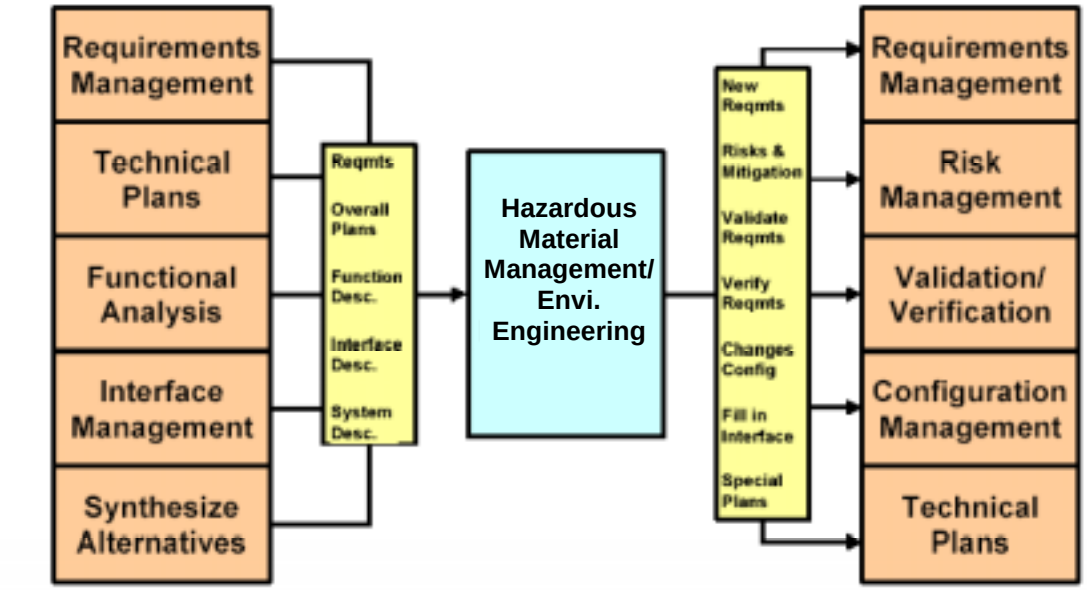


Figure 4.8-18. HMM/EE's Relationship to Other System Engineering Processes

4.8.7.4.2 Program Planning

FAA Order 1050.17 Airway Facilities Environmental Compliance Program implements the overall program for environmental compliance at FAA facilities. Each Region in the FAA has an Environmental Compliance Plan (ECP). The ECP is designed to identify and address compliance requirements in 19 environmental areas for all facilities, and therefore all systems within a region.

In addition to FAA Order 1050.17, FAA Order 4200.2, Utilization and Disposal of Excess and Surplus Personal Property, and AMS Section 2.8, Removing an Obsolete Solution, provide the requirements and framework for developing and implementing system-specific disposal plans for obsolete systems. These disposal plans are part of the Integrated Program Plan appendices; see Paragraph 4.2.2.1, Introduction to the Integrated Program Plan.

4.8.7.4.3 Products

Additionally, it is recommended that, through the HMM/EE process, a program have the capability to produce an inventory of the hazardous materials fielded equipment may contain. This information has many purposes, including, but not limited to:

- Ensuring protection of the environment and surrounding communities
- Ensuring regulatory compliance during the program's operational life
- Supporting the safety of personnel working with equipment
- Supporting disposition/disposal efforts when obsolete equipment is removed from service

4.8.7.5 References

1. FAA Order 1050.17 Airway Facilities Environmental Compliance Program
2. FAA Order 4200.2 Utilization and Disposal of Excess and Surplus Personal Property
3. AMS Section 2.8 Removing an Obsolete Solution
4. Order 1050.10, Prevention, Control, and Abatement of Environmental Pollution at FAA Facilities